Міністерство освіти і науки України
Національний технічний університет
«Дніпровська політехніка»

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеню бакалавра

Студента **Піцика Івана Віталійовича**

академічної групи *125-20-2*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему Методи реалізації захисту корпоративної пошти на платформі Gmail

Керівники	**Прізвище, ініціали**	**Оцінка за шкалою**		**Підпис**
		рейтинговою	**інституційною**	
кваліфікаційної роботи	к.ф.-м.н., проф. Гусєв О.Ю.			
розділів:				
спеціальний	ст.викл. Тимофєєв Д.С.			
економічний	к.е.н., доц. Пілова Д.П.			
Рецензент				
Нормоконтролер	ст. викл. Мєшков В.І.			

Дніпро 2024

ЗАТВЕРДЖЕНО:
завідувач кафедри
безпеки інформації та телекомунікацій
_____д.т.н., проф. Корнієнко В.І.

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу ступеня бакалавра

студенту Піцик Іван Віталійович **академічної групи** ***125-20-2***
(прізвище ім'я по-батькові) (шифр)

спеціальності *125 Кібербезпека*
(код і назва спеціальності)

на тему Методи реалізації захисту корпоративної пошти на платформі Gmail

затверджену наказом ректора НТУ «Дніпровська політехніка» від 23.05.2024 № 469-с

Розділ	**Зміст**	**Термін виконання**
Розділ 1	Розглянути види сервісів корпоративної пошти та види і збитки від загроз	04.06.2024
Розділ 2	Запропонувати методи захисту корпоративної пошти та проаналізувати їх ефективність	18.06.2024
Розділ 3	Розглянути економічну доцільність впровадження інформаційної безпеки	18.06.2024

Завдання видано _____ Олександр ГУСЄЄВ
(підпис керівника) (ім'я, прізвище)

Дата видачі: 15.01.2024р.

Дата подання до екзаменаційної комісії: 28.06.2024р.

Прийнято до виконання _____ Іван ПІЦИК
(підпис студента) (ім'я, прізвище)

РЕФЕРАТ

Пояснювальна записка: 87 с., 37 рис., 7 додатків, 35 джерел.

Об'єкт дослідження: корпоративна пошта Gmail Google workspace.

Предмет дослідження: методи реалізації захисту корпоративної пошти на платформі Gmail.

Мета кваліфікаційної роботи: підвищення рівня захищеності корпоративної електронної пошти засобами Google workspace.

Методи дослідження: порівняння, аналіз, опис

В першому розділі було розглянуто поняття та види корпоративної пошти, її архітектуру, варіанти сервісних платформ, які надають послуги отримання доменів. Проаналізовано види сервісних платформ корпоративної пошти та розглянути види, ефективність та збитки від різних видів загроз електронної пошти.

В другому розділі було запропоновано впровадження вдосконалених методів захисту корпоративної пошти в Google workspace за допомогою використання розробленого коду. Запропоновано рекомендації щодо захисту елементів сервісу корпоративної пошти шляхом впровадження протоколів безпеки, шифрування даних та сканування вкладень.

В третьому розділі було розглянуто економічну доцільність впровадження інформаційної безпеки, капітальні та експлуатаційні витрати, а також можливі щорічні витрати. Було доведено, що впровадження корпоративної пошти є мало витратним в порівнянні з можливими збитками та має мінімальний термін окупності та повернення інвестицій

КОРПОРАТИВНА ПОШТА, ФІШИНГ, ПРОТОКОЛИ БЕЗПЕКИ, СИСТЕМНЕ АДМІНІСТРУВАННЯ, SPF, DKIM, DMARC

ABSTRACT

Explanatory note: 87 p., 37 figures, 7 appendices, 35 sources.

Object of research:Corporate mail Gmail Google Workspace.

Subject of research: Methods for implementing corporate email security on the Gmail platform

The purpose of the qualification work is to study modern approaches to protecting corporate email in Google Workspace, and to develop a set of effective methods for ensuring information security, minimizing the risks of cyber threats, increasing the level of security of electronic document management in the organization, as well as assessing the economic feasibility of implementing these methods.Research methods: comparison, analysis, description.

The first section of the report examined the concept and types of corporate email, its architect, advantages compared to regular email, and options for service platforms that provide domain acquisition services. The types of threats and statistical data on the number and damage of each threat were discussed

In the second section, we propose the implementation of improved methods for protecting corporate email in Google Workspace by using the developed code. An effective approach to protecting corporate email information by means of system administration and implementation of security protocols is proposed.

The third section examined the economic feasibility of implementing information security, capital and operating costs, as well as possible annual costs. It was proved that the implementation of corporate email is low-cost compared to possible losses and has a minimum payback period and return on investment.

CORPORATE EMAIL, PHISHING, SECURITY PROTOCOLS, SYSTEM ADMINISTRATION, SPF, DKIM, DMARC.

СПИСОК УМОВНИХ СКОРОЧЕНЬ

2FA- 2-Factor Authentication;

DKIM- DomainKeys Identified Mail;

DLP- Data Leak Prevention;

DMARC- Domain-based Message Authentication, Reporting, and Conformance;

DNS- Domain Name System;

E2EE- End-to-End Encryption;

GW- Google workspace ;

IMAP- Internet Message Access Protocol;

PEM- Privacy-Enhanced Mail;

POP- Post Office Protocol;

RSA- Rivest, Shamir and Adleman;

SMTP- Simple Mail Transfer Protocol;

SPF- Sender Policy Framework;

OAEP- Optimal Asymmetric Encryption Padding;

TFA- Two-Factor Authentication;

WP- Whaling Phishing;

ЗМІСТ

ВСТУП

Електронна пошта є однією з найважливіших функцій у сфері бізнесу завдяки доступу до Інтернету як для малого, так і для великого бізнесу. Розвиток електронного документообігу, необхідність швидкого обміну інформацією для оптимізації робочих процесів призвели до того, що більшість організацій перейшли на корпоративну електронну пошту.

Успішність роботи компаній залежить від можливості оптимізувати робочі процеси таким чином, щоб повноцінне спілкування та обмін інформацією під час виконання повсякденних завдань співробітників компанії були найбільш ефективними при мінімально витраченому часі. Вимоги сьогодення, щодо залучення працівників до робочого процесу поза межами єдиного приміщення, та й навіть поза межами країни, лише пришвидшили потребу інформаційного обміну засобами електронного зв'язку.

Захист електронної та корпоративної пошти є важливим етапом захисту даних для компанії, яка використовує послуги корпоративної пошти, як основний інструмент для передачі інформації між компанією та користувачами або між співробітниками. У сучасних умовах стрімкого розвитку інформаційних технологій та зростаючої кількості кіберзагроз, питання забезпечення безпеки корпоративної пошти набуває особливої актуальності. Комплексний підхід до захисту електронної пошти включає в себе впровадження сучасних технологій шифрування, автентифікації та виявлення загроз, а також регулярне навчання персоналу з питань інформаційної безпеки.

Актуальність роботи полягає у необхідності застосування методів захисту електронної пошти. Адже, як показує статистика, атаки на електронну пошту приводять до збитків в мільярди доларів щорічно.

Об'єкт дослідження: корпоративна пошта Gmail Google workspace .

Предмет дослідження: методи реалізації захисту корпоративної пошти на платформі Gmail.

Мета кваліфікаційної роботи: підвищення рівня захищеності корпоративної електронної пошти засобами Google workspace .

Постановка задачі:

- проаналізувати види сервісних платформ корпоративної пошти;
- розглянути види, ефективність та збитки від різних видів загроз електронної пошти;
- запропонувати заходи щодо підвищення захищеності щодо корпоративної пошти шляхом застосування вбудованих механізмів захисту платформи Gmail.

РОЗДІЛ 1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Використання та ризики електронної пошти

Захист електронної пошти- це дії, спрямовані на запобігання порушенням безпеки обміну даними через поштові сервіси та захист облікових записів і повідомлень, а також конфіденційних і персональних даних.

Корпоративна електронна пошта стала важливим інструментом для компаній та організацій. Вона допомагає залучати клієнтів, відстежує листування з підрядниками і партнерами, дозволяє обмінюватися важливими документами, макетами та іншими файлами, а також виступає в ролі автовідповідача, що гарантує своєчасне отримання важливої інформації. Це також допомагає відокремити особисту переписку від службової, щоб максимально відокремити співробітників від роботи. Крім того, корпоративна електронна пошта дозволяє керівництву регулювати потік листування між співробітниками, організовувати потік інформації і мінімізувати ризики, пов'язані з факторами, властивими людській природі.

Електронна пошта дозволяє надсилати інформацію, коли вона за допомогою спеціальних програм закодована в найбільш зручну для передачі форму і не потребує повторного набору, якщо це документ або інша інформація, яка знаходиться в комп'ютері або комп'ютерній мережі. Вона також більш зручна для одержувача, оскільки одержувачу не потрібно переписувати або роздруковувати зміст електронного повідомлення. Користувач може вільно використовувати будь-яку інформацію, надану в її теперішньому вигляді, або модифікувати її, і все це без необхідності передруковувати інформацію.

Електронна пошта зручна тим, що потребує мінімальної підготовкидля її використання і є дешевшою, ніж інші способи передачі інформації, такі як звичайна пошта, факс або телефон. Вона дозволяє обмінюватися інформацією в режимі реального часу, використовуючи різні формати, що робить передачу інформації досить швидкою і зручною, усуваючи таким чином необхідність передруковувати інформацію, яку користувач вже набрав на комп'ютері. Вона дозволяє працювати в спільному просторі, використовуючи інформацію,

актуальну на момент обміну даними, дозволяє вчасно синхронізувати необхідні данні і при цьому дає змогу працювати з будь- якого місця. Все це дозволяє оптимізувати швидкий доступ до необхідної інформації, створює можливість ефективно керувати робочими процесами у співпраці з командою при мінімізації витрат.

Оскільки використання електронної пошти в основному пов'язане з використанням Інтернету, можна сказати, що це передбачає найнижчі можливі витрати на передачу інформації після початкових витрат на підключення до Інтернету. Дзвінки та чати не оплачуються, а єдиною витратою є підключення до Інтернету.

При наявності значних переваг при використанні електронної пошти неможна ігнорувати і ризики, що виникають у користувачів при обміні будь-якими даними. Загроза витоку конфіденційної та особистої інформації, поширення інформації за межами внутрішнього використання з метою крадіжки даних, хакерські атаки можуть призвести до від простих фінансових втрат до знищення бізнесу в цілому.

Витік інформації може бути умисним - коли хтось із працівників спеціально перенаправляє інформацію за межі корпоративної спільноти чи випадковими – коли інформація помилково направляється на чужу електронну адресу. Також, «піратами сьогодення» є хакерські атаки, що призводять до отримання несанкціонованого доступу до баз даних підприємств та організацій, наносячи ділові та фінансові збитки бізнесу. Не менш небезпечними є комп'ютерні віруси та спам-повідомлення

Враховуючи те, що починаючи з періоду пандемії COVID 19, а далі і з початком повномасштабного вторгнення багато компаній перейшли на віддалений режим роботи, що призвело до обміну інформацією за допомогою використання засобів електронної мережі. І це стосується не тільки офісних працівників на території України, а і у всьому світі. Такі зміни в роботі привели до збільшення кількості користувачів, і як наслідок, у зв'язку з слабким захистом або та безпечністю співробітників, зросла і кількість шахрайських дій в мережі.

Тож, на сьогоднішній день, стоїть завдання поєднати ефективне управління компанією при високому рівні комунікації працівників та створити надійний захист інформації, що є в мережі від зовнішніх чинників та несанкціонованого доступу до інформації.

1.2 Види та особливості сервісних платформ корпоративної пошти

На сьогоднішній день існує велика кількість сервісних платформ, які надають можливість створення корпоративної пошти, при цьому кожен з них має свої функції, свої плюси та свої мінуси.

Найдешевшим варіантом є хостинг через хостингові компанії, що дозволяють створити пошту з вашим індивідуальним доменом, при мінімальних затратах в розмірі приблизно 2 долари в місяць, при цьому пропонуючи мінімум послуг, що значно поступаються сервісам, які надаються іншими компаніями.

Таким чином перевагою цього варіанту є лише ціна, а втратою є відсутність доступу до додаткових видів послуг, що дозволяють мінімізувати витрати робочого часу співробітників за рахунок отримання широкого доступу до швидкого обміну інформацією на зручних та захищенихплатформах.

Більш вже потужним сервісом є Microsoft 365 Business який надає можливість на базовій версії для бізнесу використання сервісів Microsoft такі як LinkedIn, Microsoft Teams, Skype тощо. Microsoft 365 Business Standard об'єднує всі необхідні функції розміщеної служби електронної пошти - надсилання та отримання електронної пошти, користувацькі доменні адреси, спам і запобігання втраті даних– разом із програмами Office, якими ваші співробітники щодня користуються на роботі. На відміну від багатьох конкуренті Microsoft 365 Business є не хмарним, а серверним, що полегшує роботу на офісі, але ускладнює роботу при переведені компанії на дистанційний режим. Також вартість послуг із власним електронним доменом починається з 20 доларів за базову версію, що є високою ціною в порівнянні с конкурентами, враховуючи обсяг послуг, що надаються.

Для малого бізнесу існують бюджетні сервіси корпоративної пошти, один із найпопулярніших є Zoho Workplace яка пропонує розміщену електронну пошту,

календарі та контакти, а також власні програми Zoho для спілкування та співпраці: WorkDrive (для хмарного сховища), Writer, Sheet і Show (для створення та спільної роботи над документи, електронні таблиці та презентації) і Cliq (для командного чату). Але найголовнішим фактором популярності є те, що якщо у компанії п'ять чи менше співробітників, вона надає можливість безкоштовного використання усіма функціями та програмами, доменом та усім іншим

Коли додається шостий користувач, за нього прийдеться платить всього за 1 долар США на місяць або ж від 4 дол. США за користувача на місяць за стандартний план, який включає розміщення електронної пошти для кількох доменів, 30 ГБ пам'яті для електронної пошти та 10 ГБ спільного хмарного сховищами користувача.

Але також існують і мінуси: невелика підтримка системного адміністрування та безпеки, не підтримка великої кількості протоколів та відсутність можливості обмеження прав користувача, що робить Zoho Workspace ризиковим для використання великими компанія з важливою конфіденційною інформацією.

Найпоширеніший і найшвидший спосіб створити власну корпоративну електронну пошту - скористатися сервісом Google workspace (GW). Сервіс пропонує безкоштовну версію для тестування корпоративної пошти на місяць, що дозволить зрозуміти чи достатній рівень послуг надається компанією для ведення певного виду бізнесу і чи дозволить такий рівень послуг покращити ефективність роботи цього бізнесу за рахунок користування цією корпоративною поштою. Користувачі можуть отримувати доступ до персоналізованих корпоративних адрес електронної пошти, служб електронної пошти Gmail, а також зустрічей, чату, дисків, документів, електронних таблиць тощо.

При цьому корпоративна пошта захищена Google та вона надає можливість переносу всього об'єма інформації з особистої електронної пошти на корпоративну. Корпоративна пошта Google підходить до кожного виду бізнесу індивідуально. Наприклад, якщо у компанії менше 5 користувачів, кожен отримує 1 ТБ пам'яті. Базова версія коштує 5 доларів на місяць та має доступ до всіх

сервісів Google, 2 ТБ спільного сховища та включає в себе базові системи та функції безпеки та адміністрування. Для більш обширного функціоналу та можливостей в сферах безпеки та адміністрування є можливість придбання пакет версії Enterprise яка надає більш продвинуті функції безпеки і контролю для необмеженого числа користувачів.

GW є сервісною платформою для співпраці, який вибирають багато стартапів, і це не без причин. Почати роботу легко. Ви можете збільшувати кількість користувачів і функцій у міру зростання. Він має більш зручний інтерфейс, ніж деякі його конкуренти, особливо для малого бізнесу на початковому етапі роботи.

Однією з незрівнянних переваг Google workspace є його здатність допомагати зростаючим підприємствам безперешкодно масштабуватися, підвищуючи безпеку та загальну ефективність, що зрештою сприяє зростанню бізнесу. GW пропонує надійні функції безпеки для захисту від кіберзагроз, як Фішингу або витік даних , забезпечуючи безпеку ваших данихпо мірі розширення вашого бізнесу.

Крім того, Google workspace використовує штучний інтелект (ШІ), щоб підвищити продуктивність різними способами, наприклад швидке відображення відповідного вмісту та допомога у написанні електронних листів. Ця інтелектуальна допомога може заощадити дорогоцінний час і оптимізувати робочі процеси, дозволяючи вашій команді зосередитися наосновній бізнес-діяльності.

Принцип роботи електронної пошти Gmail від відправлення листа одним користувачем до отримання іншим проходить в декілька етапів:

1. Відправник створює та відправляє лист на своєму аккаунті Gmail.

2. Лист надсилається через сервера SMTP (Simple Mail Transfer Protocol), що є програмним забезпеченням для збереження, обробки та доставки вхідних та вихідних листів. Спочатку поштовий клієнт або сервер відправника встановлює з'єднання з SMTP-сервером одержувача та надає необхідну інформацію, наприклад адресу електронної пошти одержувача. Потім SMTP-сервер обробляє цю інформацію та перевіряє адресу одержувача, щоб прийняти

електронний лист чи ні. Його також можна назвати сервером вихідної пошти.

3. Після цього лист потрапляє на сервера Google, де зберігається в базах даних. Для доставки використовуються два протокола: IMAP і POP. Ці два протоколи схожі за дією але відрізняються в деталях. POP (Post Office Protocol) зберігає лист на вашому комп'ютері та в базі даних Google вашого провайдера та не дозволяє бачити лист з інших пристроїв, що робить неможливим потрапляння в руки шахраїв при взломі. В той же час IMAP (Internet Message Access Protocol) більш швидкий, зберігається в хмарі та дає можливість продивлятись лист на різних пристроях, що корисно коли у користувача декілька пристроїв, але робить неможливим автоматичне зберігання та перегляд при відсутності інтернету.

4. Коли одержувач перевіряє свою пошту, його запит на доступ до нових листів проходить через сервер IMAP/POP. Сервер IMAP/POP завантажує листи з бази даних збереження листів і відправляє їх на клієнтський пристрій одержувача. Він отримує електронного листа у своєму акаунті Gmail через інтерфейс Gmail. Весь процес доставки забезпечується протоколами, які гарантують надійність і безпеку передачі даних.

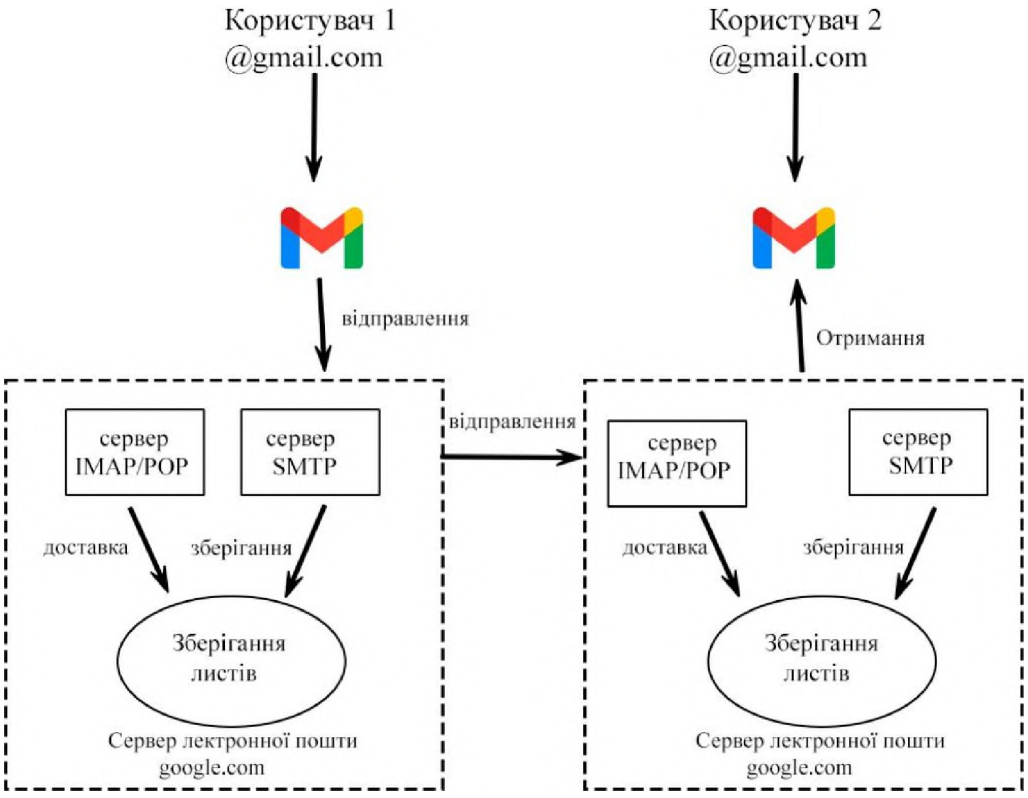

Рисунок 1.1 – Архітектура роботи пошти Gmail

1.3 Основні категорії загроз електронної пошти

За допомогою кібератак шахраї використовуючи методи соціальної інженерії в електронних листах та повідомленнях, змушують людей власноруч передавати особисті дані, такі як паролі та фінансову інформацію, або виконувати певні дії, такі як завантаження зловмисного програмного забезпечення або банківські перекази приводячи до збагачення кіберзлочинців. Ці схеми стали складними та цілеспрямованими, створили значні загрози як для простих громадян так і для малого і великого бізнесу.

Спам-фільтри вловлюють більшу частину загрозливих листів, але нові, більш витончені методи все ще проникають у вхідні листи. Більшість людей знають про існування кібератак, і багато компаній проводять тренінги та симуляції, щоб навчити співробітників виявляти шкідливі електронні листи та повідомлення.

Проте, незважаючи на ці зусилля, шахраї продовжують успішно здійснювати подібні кіберзлочини, а використання атак на електронну пошту як і раніше зростає, і кіберзлочинці постійно змінюють свою тактику, щоб обійти існуючі заходи боротьби з подібними атаками , а організаціям необхідно постійно вдосконалювати свої методи захисту.

1.3.1 Фішинг

Фішинг є найпоширенішою формою кіберзлочинності. Кожен день кіберзлочинці надсилають 3,4мільярда електронних листів, які створенні так, ніби вони надходять від надійних відправників. Це понад трильйон Фішингових листів на рік, що приблизно 1,2% усього трафіку електронної пошти в усьому світі. Фішинг дуже простий у використанні і не вимагає особливих технічних знань, але для ефективної атаки необхідно лише добре розбиратися в психології людини і зібрати потрібну інформацію. Через це більшість атак є Фішинговими, або починаються з Фішингу, для подальшого отримання більш важливої інформації для взлому системи. Фішинг ділиться на підрозділи згідно з ціллю та методом атаки, основними з них є звичайний, цільовий та вейлінг Фішинг. Отже розглянемо кожен з них

Фішинг електронної пошти- це найбільш поширений тип атак. Використовується методом «розпилюй і молись» і зазвичай використовується, коли хакери, які видають себе за довірених людей або організації, надсилають велику кількість електронних листів на всі відомі адреси. Ці електронні листи можуть містити шкідливі посилання або програмне забезпечення, а також вміст, який змушує жертв передавати свої особисті дані зловмисникам.

Фішингові шахраї стають набагато активнішими під час епідемій і воєн, використовуючи нестабільність і страх людей для досягнення своїх цілей. Під час таких криз, коли люди шукають надійну інформацію та підтримку, шахраї використовують соціальну інженерію для маніпулювання конфіденційною інформацією та її крадіжки.

Під час пандемії COVID-19 кількість Фішингових атак значно зросла. Шахраї відправляли велику кількість електронних листів під виглядом офіційних повідомлень від медичних установ і державних структур, пропонуючи підроблені ліки, тестуючи їх або допомагаючи в їх виготовленні. Вони використовували паніку та тривогу, щоб змусити людей розкривати свої особисті дані або встановлювати шкідливе програмне забезпечення на свої пристрої.

Аналогічним чином під час війни в Україні, почастішали Фішингові атаки. Зловмисники використовували тему війни для поширення підроблених запитів на благодійність, пропозиції допомоги та іншої інформації, викликаючи емоційну реакцію людей, змушуючи їх розкривати фінансові дані або переводити кошти на підроблені рахунки. Війна створює хаос і невизначеність, знижує пильність людей і збільшує успіх подібних атак. Враховуючи те, що на початку війни за рахунок допомоги країн- партнерів, держава намагалася фінансово допомогти незахищеним верстам населення, громадянам, що втратили своє майна, тощо, виплачуючи фіксовану матеріальну допомогу на карткові рахунки, злочинці почали використовувати підробні схеми нібито повторних виплат. Військові дії на території України призвели до зубожіння мирного населення, що дозволило злочинцям використовувати тяжке фінансове становище для зниження пильності громадян.

Таким чином, епідемії та війни створюють ідеальні умови для Фішингових шахраїв, які використовують кризи для маніпулювання емоціями людей та додаткових заходів безпеки. Наступний графік, що створений в результаті аналізу щорічних втрат від Фішингу дозволяє наглядно побачити зріст втрат лише за останні 4 роки.

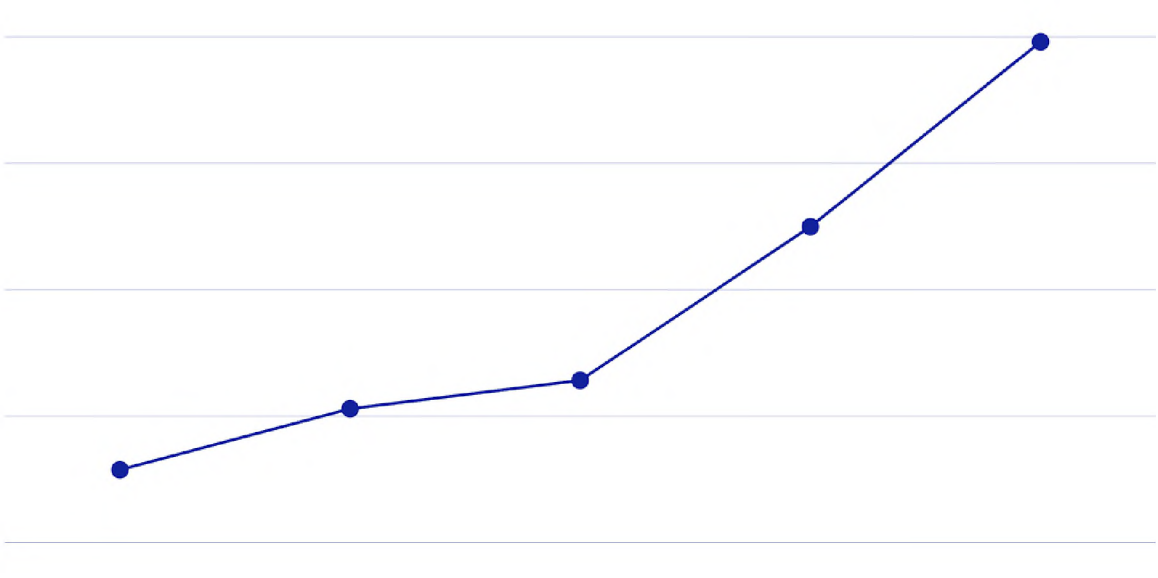

Рисунок 1.2 – Щорічні збитки від Фішингових атак

На перший погляд, Фішинг - це лише електронний лист із підозрілим вмістом, який нічого не робить, поки користувач сам не вчинить певну дію, яка завдасть в подальшому йому шкоди. Але ця людина цього не зробить, правда? Насправді, ні. Незважаючи на те, що ми вважаємо себе розумними істотами, ми часто покладаємось на інстинкти та дії, які сприяють полегшенню виживання. Крім того, простота всьому світу (особливо в інших частинах Західної Африки та в Азії). Ці шахрайства все частіше називають «шахрайством з авансовими платежами».

У класичному нігерійському шахрайстві користувач отримує електронний лист від шахрая з проханням допомогти переказати грошові активи за кордон. За допомогу йому буде запропонована частина грошей, якщо він погодится. Але потім, якщо людина довірилась і перевела вказані йому гроші, шахраї відразу

пропадають або продовжують просити переводити суму на оплату комісії або зборів, аж допоки людина не зрозуміє що ніяку «винагороду» він не отримає.

Сценарії бувають різноманітні- від нігерійського принца с замороженими активами для розморожування яких треба деяка частина грошей до вигаданого покійного родича без прямих спадкоємців, де власник листа є єдиним живим далеким родичем, що вказаний в заповіті як правонаступник спадщини. Для цього часто вказуються родинні зв'язки спадкодавця з родичами третього-четвертого покоління, які могли б перебувати за кордоном і мають спільні корені рідства, що дозволяють "майбутньому спадкоємцю" розраховувати на грошову винагороду.

Багато людей, звичайно, не звернуть уваги на цей лист, але ті, хто перебуває у важкому фінансовому становищі і не має базових знань про кібергігієну, можуть легко потрапити на цю вудку. Аналітики також помітили,що шахраї активізуються під час емоційно-напружених подій, таких як епідемії та війни. У такі моменти зловмисники використовують теми, що стосуються всіх, наприклад створюють посилання на несправжні благодійні пошти допомоги, і стрес, який відчуває жертва у ці важкі часи, притупляє увагу і робить його більш вразливими до Фішингу.

Шахраї не однаково активні в період року. Останні дослідження та опитування показали, що зловмисники найбільш активні у серпні, а період з вересня по грудень вважається одним з найбільш інтенсивних в Фішингових атаках, що збігаються з сезоном святкових покупок. Згідно з опитуванням Bolster, за 3 місяці до свята припадає 35% всіх Фішингових атак. У цей період приватні особи і компанії готуються до святкування і активно здійснюють онлайн-покупки. Кіберзлочинці користуються таким рівнем активності в Інтернеті, використовуючи різні методи, такі як Фішингові електронні листи щоб обдурити нічого не підозрюючих користувачів та отримати фінансову вигоду. В серпні 2023 були зафіксовані рекордні всплески Фішингових атак, коли багато американців були у відпустці під час літніх канікул. Зокрема, дослідження, проведене компанією Bolster, виявило різке зростання числа Фішингових кампаній, пов'язаних з податками, таких як фальшиве повернення податків або

несплачені податки, як обманом змушують нічого не підозрюючого користувача натиснути на шкідливе Фішингове посилання [3].

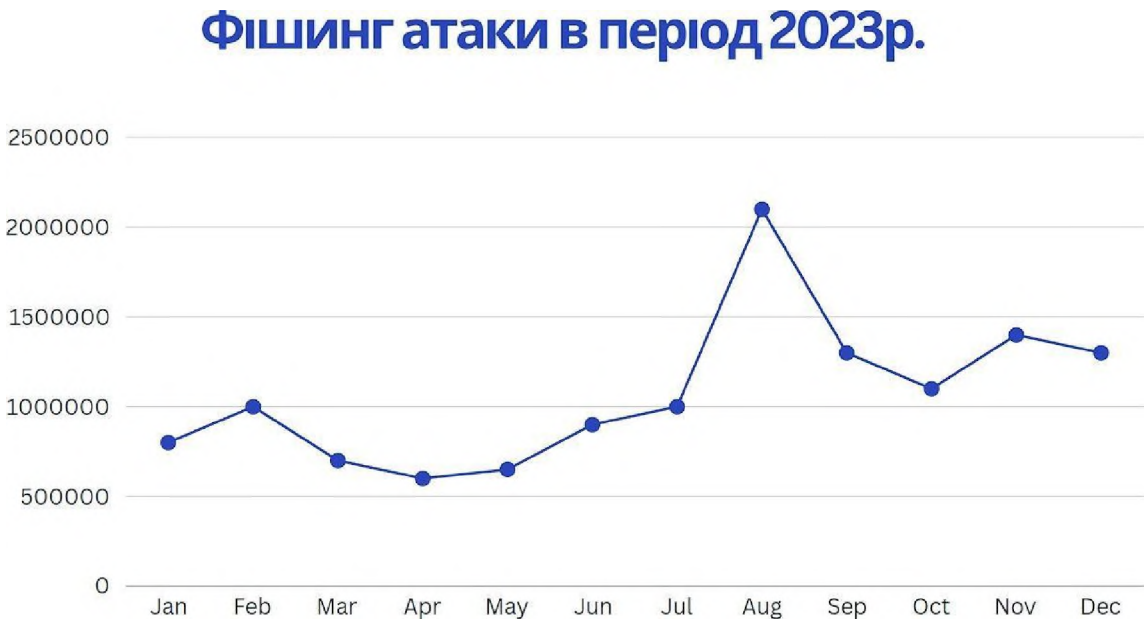

Рисунок 1.3 – Частота Фішинг атак в період одного року

Згідно статистичних даних, які приведені в статті компанії The APWG Phishing Activity Trends Reports, атаки на різні сфери діяльності відрізняються між собою як кількісною так і якісною складовою. Таким чином можна стверджувати, що кіберзлочинці не атакують різні сфери діяльності однаково [7]. Це пов'язано з унікальними характеристиками та цінністю даних у кожній області. Різні галузі, такі як фінанси, логістика, комунікації та виробництво, мають специфічні загрози та відповідно до цього мають на меті досягнення різних цілей для кіберзлочинців. Найчастіше для кібератак зловмисники вибирають фінансові установи та веб- пошту, найрідше такі атаки відносилися до засобів телекомунікації або до криптовалюти. Таким чином видно, що найуразливішою сферою діяльності, є діяльність фінансових установ, так як кількість кібератак складає майже 30% від загального обсягу. Насамперед, це пов’язано с тим, що робота фінансових установ працює по типовому принципу в багатьох країнах світу. Найчастіше, фінансові установи користуються загальними міжнародними програмами для пришвидшення та спрощення роботи на внутрішньому та міжнародному ринку. Це і дозволяє швидше підбирати ключи для злому таких програм і крім цього фінансовий бізнес приваблює злочинців великим об’ємом

фінансових потоків.

Найменш же привабливим для кіберзлочинців є кріптовалютні сервісні установи. Через специфіку роботи криптовалют сервіси є більш захищеними, на відміну від традиційних фінансових установ. Зберігання даних в блокчейн забезпечує шифрування різними криптографічними методами заради забезпечення безпеки, конфіденційності та анонімності користувача, його фінансових рахунків та транзакцій.

Цей аналіз для наочності викладено в наступній круговій діаграмі, що дозволяє в більш спрощеному вигляді ознайомитися з результатами цих статистичних даних [7].

Рисунок 1.4 – розподіл Фішингових атак між сферами діяльності

Цільовий Фішинг- це метод Фішингу, спрямований на окремих осіб або групи в організації. Це потужний варіант Фішингу, зловмисна тактика, яка використовує електронну пошту, соціальні мережі, обмін миттєвими повідомленнями та інші платформи, щоб змусити користувачів розкрити особисту інформацію або виконати дії, які спричиняють компрометацію мережі, втрату даних або фінансові втрати. У той час як тактика Фішингу може покладатися на збройні методи, які масово доставляють електронні листи випадковим особам, цільовий Фішинг зосереджується на конкретних цілях і вимагає попереднього

дослідження.

Типова Фішингова атака включає електронний лист і вкладення. Електронний лист містить інформацію, специфічну для об'єкта, зокрема ім'я об'єкта та його посаду в компанії. Ця тактика соціальної інженерії підвищує шанси того, що жертва виконає всі дії, необхідні для зараження, включаючи відкриття електронної пошти та доданого вкладення. Зловмисники витрачають багато часу та зусиль, щоб відстежити якомога більше подробиць про роботу, життя, друзів і родину одержувачів.

Переглядаючи профілі в Інтернеті та соціальних мережах на таких платформах, як Facebook і LinkedIn, фішери можуть знайти таку інформацію, як адреси електронної пошти та номери телефонів, мережу друзів, сім'ї та ділові контакти, відвідувані місця, а також такі речі, як компанія, в якій вони працюють. їїхнє становище, де вони здійснюють покупки в Інтернеті, якими банківськими послугами користуються тощо.

Використовуючи всю цю інформацію, зловмисники можуть створювати розширені профілі своїх потенційних цілей і створювати Фішингові електронні листи за допомогою методів соціальної інженерії, які персоналізовані та виглядають законними, оскільки надходять від осіб або компаній, з якими вони регулярно взаємодіють, і містять інформацію, яка може бути автентичною.

Прикладом ефективності Цільового Фішингу є новина про те, що компанія RSA втратила можливість використання двофакторної аутентифікації та конфіденційної інформації після того як зловмисник надіслав два різні Фішингові листи протягом двох днів. Два електронні листи було надіслано двом невеликим групам співробітників. Електронний лист був створений настільки добре, що обманом змусив одного зі співробітників відкрити вкладений файл Excel. Після відкриття зловмисник отримав віддалений доступ до серверу та зібрав облікові записи користувачів, адміністратора домену та служби, а потім перейшов до отримання доступу ключових високоцінних цілей, серед яких були експерти з процесів і адміністратори серверів, що не належать до IT.

Whaling Phishing (WP)- це техніка, яка використовується кіберзлочинцями, щоб замаскуватися під керівників всередині організації та безпосередньо націлюватися на посадовців та інших важливих осіб з метою крадіжки фінансів або конфіденційної інформації або доступу до комп'ютерних систем у злочинних цілях. Вейлинг, також відомий як шахрайство з Генеральним директором, схожий на Фішинг тим, що він використовує такі методи, як підробка електронної пошти, щоб обдурити цілі, щоб вони виконували певні дії, такі як розкриття конфіденційних даних або переказ грошей.

В той час як Фішингові атаки націлені на широку аудиторію, цільовий Фішинг націлений на конкретних людей- WP є більш удосконаленим варіантом цільового Фішингу, оскільки він не тільки націлений на ключових людей, але й надсилають шахрайські повідомлення від керівників або інших впливових осіб в організації. Цедодає елемент соціальної інженерії, оскільки співробітники, як правило, частіше довіряють та частіше задовольняють вимоги людей, яких вони вважають важливими.

Через специфіку атаки, що треба вивчати та відправляти від імені керівника, Whaling більш рідкісний але при успішному виконані операції шахрай отримує доступ до більш конфіденційної інформації та має можливість викрасти її на більш високу суму. В США лише за 2021 рік китобійний промисел призвів до збитків на суму 12,5 мільярдів доларів.

Одним із найвідоміших випадків WP був викрадення конфіденційної інформації Snapchat коли до одного із співробітників прийшов фальшивий лист нібито від генерального директора Еван Шпігель. В листі співробітника відділу кадрів попросили скинути весь список даних заробітної плати всіх співробітників компанії з прикріпленням до цього особистої інформації, такої як електронна пошта, номера телефону та домашні адреси. Через такий великий злив даних компанія надала всім постраждалим співробітникам два роки безкоштовного страхування від крадіжки особистих даних та виплатилаодноразову компенсацію всім працівникам.

1.3.2 Спам

Спам – це небажана електронна пошта, яка часто містить комерційні повідомлення або посилання на веб-сайти. спам-лист зазвичай надсилається великій кількості одержувачів з наміром рекламувати продукт, послугу чи ідею. Вони часто дратують і не обов'язково є зловмисними, але можуть засмітити вашу папку «Вхідні». електронні листи зі спамом можуть містити рекламний вміст, рекламу або пропозиції щодо продуктів чи послуг. Вони також можуть містити посилання на веб-сайти, де щось продається.

До поширених типів спаму належать пересилання молитовних листів, купони, вміст для дорослих, прохання про пожертви та небажані інформаційні бюлетені. Зазвичай вони мають комерційний характер і не є явно шкідливими. Але в деякий випадках під рекламним спамом може переховуватись Фішинг, який при вивчені ваших інтересів та пропозицій продуктів створює підробне посилання на сайт та викрадає ваші облікові дані.

Але навіть без зливу конфіденційної інформації Спам має велику загрозу для людей. Одним із найпопулярніших тем спаму є онлайн казино та шахрайські онлайн магазини які при замовлені товару беруть повну суму і пропадають не відправляючи товар або відправляючи не те, що замовляли.

Спам займає значну частину електронної пошти, яку отримують користувачі та організації. Витрачання часу на сортування та видалення спаму знижує продуктивність. Співробітники можуть втратити важливу інформацію серед маси непотрібних повідомлень, що додатково впливає на ефективність роботи.

Боротьба зі спамом в корпоративній пошті є одним із найдорожчих пунктів захисту. Організації змушені інвестувати значні кошти у програмне забезпечення та апаратні засоби для захисту від спаму. Це включає в себе використання фільтрів спаму, антивірусного програмного забезпечення та інших інструментів кібербезпеки, що може бути дорогим і складним у підтримці.

Також спам може діяти на людину психологічно. Постійне отримання небажаних повідомлень може викликати стрес і роздратування у користувачів. Це

також може вплинути на загальне відчуття безпеки і довіри до електронної пошти як засобу комунікації. Людина починає відчувати параною і недовіру навіть до звичайної пошти.

Навіть при тому що пошта автоматично вміє розпізнавати спам та фільтрує 99% спам листів, лише в США він призводить до збитків в десятки мільярдів доларів і ця цифра лише росте. Дослідники з Каліфорнійського університету в Сан- Дієго виявили, що онлайн-спамери заробляли в середньому близько 7000 доларів США на день, що складає приблизно 2,5 мільйона доларів США на рік [10].

Однак ця цифра може значно варіюватися залежно від виду шахрайства, з деякими зловмисниками заробляють значно менше, а інші – набагато більше. Тому через свою легкість, розповсюдженість та швидкий заробіток- спам є першою сходинкою в світі кіберзлочинності для багатьох шахраїв.

Рисунок 1.5 – річні збитки від спам листів в електронній пошті

1.3.3 Програми-вимагач

Програми-вимагачі, або по іншому Ransomware - це різновид шкідливих програм, які можуть красти, блокувати або шифрувати дані на комп'ютері

користувача. Після завершення руйнівної дії зловмисник повідомляє жертві про атаку і вимагає викуп за відновлення доступу до даних або погрожує розкриттю конфіденційної інформації. Метод, який використовує зловмисник, залежить від уподобань групи та конкретного випадку. Після успішної атаки завжди вживаються трудомісткі та дорогі дії для усунення інших ризиків, таких як відновлення доступу, відновлення файлів та витік даних клієнта. Зазвичай зловмисне програмне забезпечення встановлюється на комп'ютер користувача через атаку методом соціальної інженерії, де користувача обманом змушують натиснути на Фішингове посилання або відкрити шкідливий файл.

Після того, як програмне забезпечення потрапляє на комп'ютер, воно починає шифрувати всі доступні файли як на самому пристрої, так і на всіх мережевих ресурсах, до яких має доступ ПК.

Коли користувач намагається відкрити зашифрований файл, йому відмовляють у доступі. Системний адміністратор, отримавши повідомлення від користувача, знаходить у каталозі два файли: один з вимогою викупу, а інший з інструкціями щодо сплати цього викупу для розшифровки файлів. Після того, як файли зашифровано, єдиний спосіб повернути їх – це відновити резервну копію або заплатити викуп. Однак зараз кіберзлочинці часто пошкоджують резервні копії ще до того, як жертви дізнаються, що їх спіткало. Журнал Storage Magazine повідомляє, що понад 34% компаній не тестують свої резервні копії, а 77% із протестованих виявили, що резервні копії на стрічку не вдалося відновити. За даними Microsoft, 42% спроб відновлення з резервних копій на стрічку минулого року були невдалими.

Нові варіанти шкідливого програмного забезпечення постійно з'являються, оскільки нові кіберзлочинні угрупування вступають у «бізнес». Методи, які використовують зловмисники, постійно удосконалюються,щоб обійти традиційні заходи безпеки. Серед відомих угрупувань, які використовують ці методи, можна виділити WannaCry, GandCrab, Phobos і Cerber. Це надзвичайно успішна модель кримінального бізнесу.

Від угрупувань кожен рік тисячі компаній зазнають збитків в мільйони

доларів. Лише за 2023 рік вимагачі змогли на продажі шифрованої інформації заробити більше 40 мільярдів доларів [11]. Це є основною проблемою для всіх компаній, особливо для малого та середнього бізнесу, у яких немає планів та схем захисту від програми вимагача і тому вони частіше стають доступними цілями для кіберзлочинців.

1.3.4 Спуфінг

Спуфінг, або ж підробка- це вид кіберзлочинності, коли шахрай маскується під фізичну особу, компанію чи організацію для вчинення зловмисних дій. Кіберзлочинці використовують різні тактики, щоб підробити свою особу, починаючи від підроблених адрес електронної пошти, і закінчуючи більш складними стратегіями, як-от шахрайські IP-адреси або сервери доменних імен (DNS). При стандартних налаштуваннях електронної пошти та без сторонніх протоколів система захисту не може сама по собі автентифікувати джерело електронного листа. Таким чином, спамеру або іншим зловмисникам, відносно легко змінити метадані електронного листа. Таким чином, протоколи вважають, щоце переслав справжній відправник.

Спуфінг є одним з найстаріших кіберзлочинів в електронної пошті, який було згадано ще 1996 році, коли хакерам вдалось за допомогою фальшивих кредитних карток створити акаунти, які копіювали назву та адресу банку Америки. Потім ці акаунти використовувались для того, щоб виманювати конфіденційну інформацію у нічого не підозрюючих користувачів банку.

Шахрайство підробки с кожним роком продовжує розвиватися та має цілі атак як малого підприємства так і крупних бізнесів. Лише в США за 2023 рік збитки від спуфінгу нараховуються в більше, а ні ж в 17,3 мільярди доларів і число атак та збитків з кожним роком стає ще більшою.

1.4 Аналіз впливу загроз на бізнес

Аналізуючи отриману інформацію, можна говорити про те, що лише за 2023 рік така країна, як США, отримала збитків, завданих кібератаками, більше ніж 159 мільярдів доларів. Найбільша частка приходить на малий та середній бізнес через невисокий рівень захисту інформації по причині малих коштів, які витрачаються

на безпеку даних.

Найбільше компанії страждають від програм-вимагачів тому, що від зараження складно позбутися через специфіку атаки зараження комп'ютера, де єдиними варіантами є або заплатити викуп, або переустановлювати систему з надією на збереження інформації в хмарі.

Звичайний Фішинг, зокрема, став другою за масштабом проблемою, завдавши збитків на 40 мільярдів доларів. І хоча середній збиток на одного користувача набагато менше ні ж в цільового та вейлінг Фішингу,- беручи кількістю та відправляючи листи в кожен куток світу завдається проблема, яку не можуть вирішити на 100 відсотків ось уже як 30 років.

Рисунок 1.6 – загальний графік збитків від різних загроза один рік

З кожним роком, кібератаки стають більш складнішими, використовуючи методи дослідження соціальної інженерії злочинці за допомогою підступних методів вводять в оману слабо захищених користувачів мережі. Тому важливо приділяти особливу увагу кібергігієні та впровадженню надійних засобів захисту. Таким чином, регулярне навчання співробітників, використання багатофакторної

аутентифікації, впровадження політик обмеження даних і активне використання сучасних антивірусних і анти Фішингових інструментів - це мінімум, який необхідно зробити для захисту систем та інформації.

Важливим аспектом захисту інформації в роботі середнього та великого бізнесу є мінімізація використання особистої та перехід докорпоративної пошти.

Це дозволить зменшити ймовірність втрати інформації через слабку обізнаність співробітника в дотримані кібергігієни та дозволить скористатися надійними сервісами корпоративної пошти, що надають можливість ретельного налаштування захисту, можливість моніторингу системного адміністратора, додаткові фільтри від спаму і Фішингу та тому подібне.

Перехід на корпоративну пошту також сприяє покращенню комунікації всередині організації, забезпечуючи єдину платформу для обміну інформацією.

Це сприяє прозорості процесів, швидкому обміну даними та співпраці між різними відділами. Корпоративна пошта може бути налаштована відповідно до потреб компанії, включаючиналаштування рівнів доступу, що обмежують доступ до певної інформації лише для авторизованих користувачів.

Таким чином, впровадження корпоративної пошти є стратегічним кроком для забезпечення надійного захисту інформації, підвищення ефективності бізнес-процесів та створення безпечного середовища для зберігання та передачі даних. Це дозволяє компаніям не лише захистити свої дані, але й покращити взаємодію між співробітниками, оптимізувати робочі процеси та відповідати сучасним вимогам кібербезпеки.

У спеціальному розділі необхідно впровадити захист корпоративної пошти в Google workspace . Існує велика кількість методів забезпечення захисту і безпеки користувачів та інформації, наприклад налаштування функцій безпеки та адміністрування, шифрування інформації при відправці листа, підключення протоколів безпеки, проведення регулярних тренінгів для співробітників з метою підвищення їх обізнаності про кібербезпеку та тому подібне.

1.5 Висновок до першого розділу

У першому розділі було детально розглянуто концепцію корпоративної електронної пошти, її структуру та функціональні можливості, що надаються платформою Google workspace . Описано різні види корпоративної пошти, такі як інтегровані поштові системи, які забезпечують ефективну комунікацію всередині організації та між її підрозділами. Також було висвітлено ключові переваги використання таких систем, зокрема підвищення продуктивності співробітників через швидку і надійну доставку повідомлень та можливості детального налаштування безпеки шляхом адміністрування

Було підкреслено переваги корпоративної пошти, зокрема у сфері підвищеної безпеки, надійності, централізованого адміністрування та можливості інтеграції з іншими корпоративними сервісами. Розглянуто основні загрози, з якими стикається корпоративна пошта, включаючи Фішинг, спам, програми-вимагачі та спуфінг. Ці загрози було детально проаналізовано, що дозволило оцінити їх вплив на безпеку та функціональність поштових систем.

РОЗДІЛ 2. СПЕЦІАЛЬНА ЧАСТИНА

2.1 Налаштування захисту Google workspace внутрішніми методами безпеки

Google workspace має ряд важливих функцій безпеки – однак багато з них не ввімкнено за замовчуванням, тому для створення більш безпечного користування корпоративною поштою їх потрібно обов'язково ввімкнути та налаштувати. Також треба мати на увазі що велика кількість функцій доступні в пакеті версії Enterprise Plus який надає додаткові функції налаштування безпеки та адміністрування. Доступ до всіх цих налаштувань здійснюється через портал адміністратора Google workspace , який знаходиться за адресою admin.google.com.

Першочергово треба встановити обов'язкове налаштування двофакторної аутентифікації (2FA або TFA), який є технічним терміном для процесу, згідно з якого користувач повинен підтвердити свою особу двома унікальними способами, перш ніж йому буде надано доступ до системи. Традиційно користувачі покладаються на системи автентифікації які вимагають від них надати унікальний ідентифікатор, наприклад адресу електронної пошти, ім'я користувача або номер телефону, а також правильний пароль. 2FA розширює цю безпеку, додаючи додатковий крок до процесу автентифікації, найчастіше вимагаючи від користувача введення одноразового токена, який динамічно генерується та доставляється на пристрій, до якого має доступ лише користувач, наприклад його телефон або особиста електронна пошта. Двофакторна аутентифікація важлива тому, що паролі можуть бути скомпрометовані різними способами, включаючи Фішингові атаки, витоки даних або зломи. Однак, навіть якщо зловмисник отримає пароль, 2FA потребує додаткового коду а отже тільки паролю буде недостатньо для доступу до облікового запису.

В стандартних налаштуваннях двофакторна аутентифікація є лише рекомендацією, кожен користувач зможе включити лише за власним бажанням, що небезпечно при роботі з важливими даними. Для встановлення обов'язкового включення TFA треба в пункті «Аутентифікація», щоб було вказано обов'язкове включення 2FA та відправлення коду на СМС або електрону пошту.

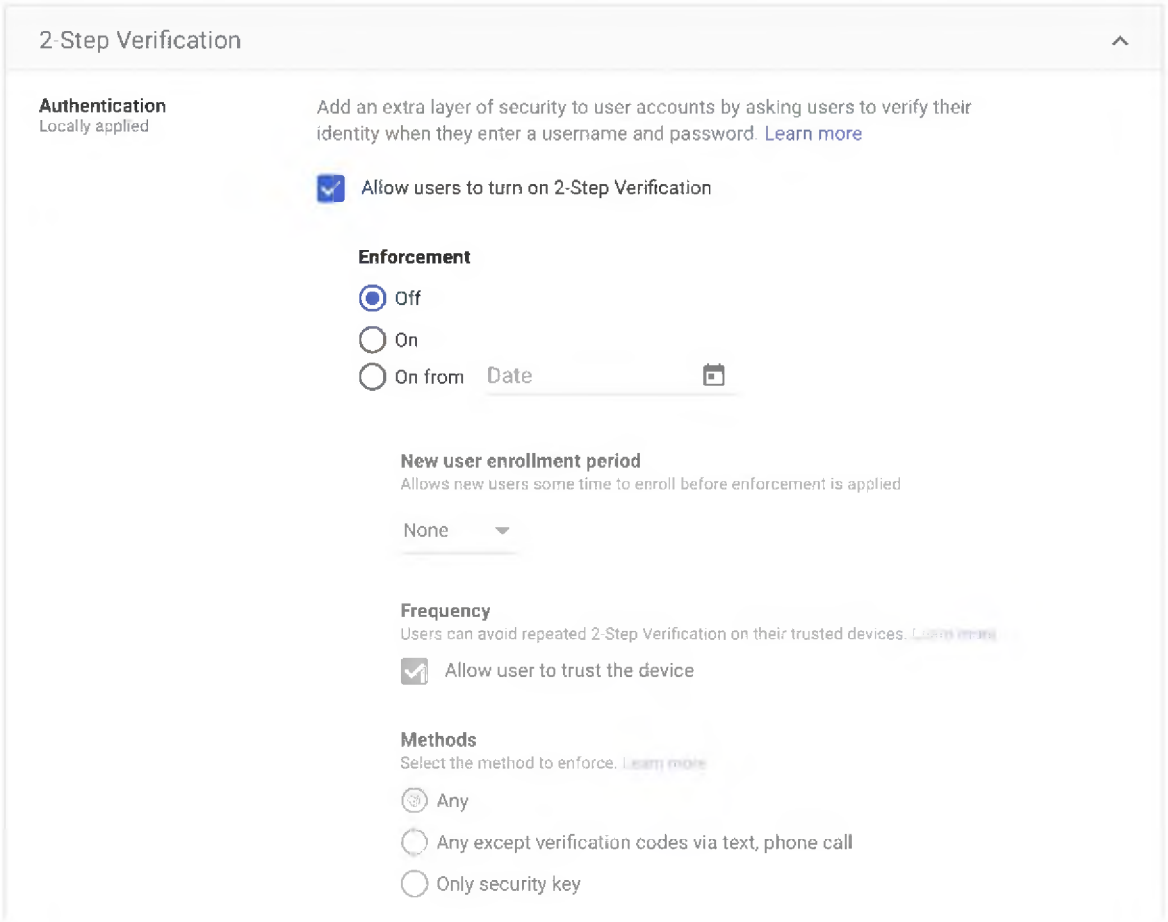

Рисунок – 2.1 Включення обов'язкової двофакторної аутентифікації

Наступним важливим пунктом безпеки є впровадження більш складних та стійких паролів. Безпека паролів є однією з найважливіших складових кібербезпеки. Ось чому довжина пароля має значення і чим довший пароль, тим він безпечніший. Довгі паролі мають більшу кількість можливих комбінацій символів, що значно ускладнює їх злом методом "грубої сили" (brute force).

За замовчуванням встановлено мінімальну довжину в 8 символів, що не є достатньо безпечною довжиною, особливо якщо користувач використовуватиме популярні паролі та слова. Пароль довжиною в 8 символів можливо методом перебору можливо взломать максимум за 5 хвилин, пароль довжиною в 12- за місяць. Але для взлому пароля методом перебору з випадковими 16 символами та використанням нижнього та верхнього регістру потрібно потратити вище мільйона років.

Для встановлення мінімальної довжини потрібно в розділі "управління паролями" встановити нову мінімальну довжину. Також в цьому розділі є пункт

налаштування часу існування після якого пароль стає неактуальним і його потрібно буде змінювати, але при довжині в 16 та включеній 2FA захиствходу в обліковий запис вже є достатньо захищений і тому цей пункт не є обов'язковим для стабільної безпеки.

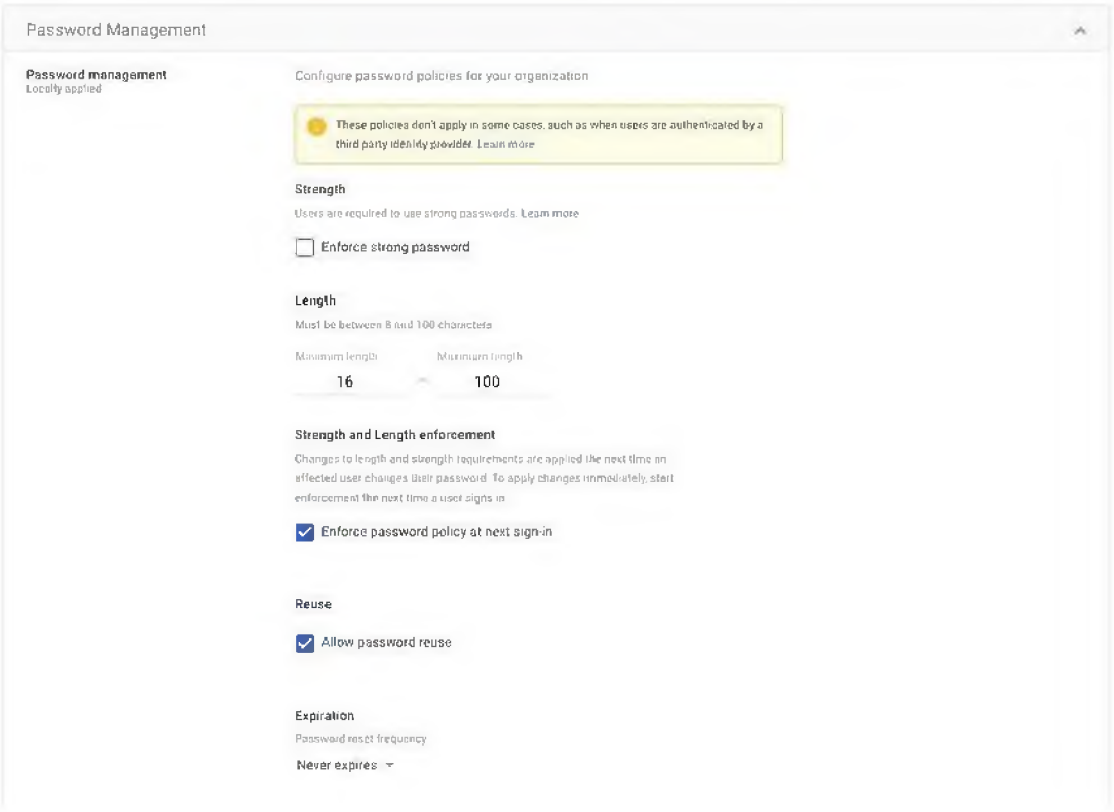

Рисунок 2.2 – Зміна мінімальної довжини пароля

Наступні кроки допоможуть захистити корпоративну пошту від Фішингових атак та є унікальними для Google workspace . Один з них- це впровадження ефективного фільтру, який за допомогою додаткових перевірок на спам та підозрілість листа і буде відправляти їх у "Вхідні" якщовсе нормально або ж в "Спам" якщо перевірка виявила проблему. Для включення додаткового фільтру потрібно в розділі "Spam, Phishing and Malware" потрібно змінити "OFF" (виключено) на "ON" (включено).

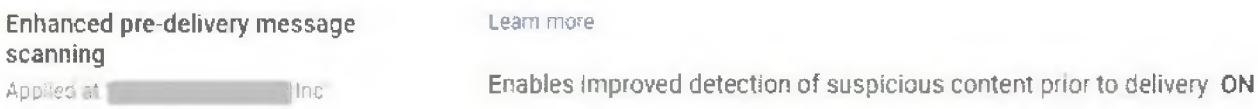

Рисунок 2.3 – впровадження додаткових фільтрів для захисту від Фішингу.

Але іноді додатковий фільтр може помилково закинути звичайний лист в папку “Спам” і навіть якщо ви прочитаєте його всі наступні посилання від цього користувача будуть помічатись як “Спам” або ж навпаки- Фішинг або спам, який був декілька разів відправлений з одного й того самого відправника, не потрапляє у відповідну папку. Тому в налаштуваннях є можливість створення Білого та Чорного списку.

Білий список- список IP-адрес, які адміністратор визначає, як схвалені для надсилання пошти на домен компанії. Після того, як адресу внесуть в білий список, повідомлення, які надходять із цієї IP-адреси, не потраплятимуть у мітку спаму. Однак користувачі, які отримують електронну пошту з цієї IP- адреси, все одно побачать у цих повідомленнях банер із застереженням Gmail про можливу небезпеку листа.

Прямою протилежністю білого списку є чорний список- список електронних адрес, з яких блокується надсилання пошти до організації чи домену. Адміністратори можуть блокувати домени або окремих користувачів за допомогою “параметра заблокованих відправників”. Крім того, користувачі можуть створити фільтр у своїх поштових скриньках для автоматичного надсилання повідомлень від певних користувачів або списків електронної пошти до кошика. Користувачі також повинні повідомляти про небажані повідомлення, як про спам, що допомагає спам- фільтрам Gmail виявляти майбутні спам-повідомлення. Крім того, блокування через IP- адресу як і одного користувача так і нових користувачів які відправляються с заблокованого пристрою. А отже, якщо шахрай після попадання в чорний список вирішить створити новий обліковий запис- листи з нього будуть автоматично потрапляти в папку “Спам”.

Для створення білого та чорного списку потрібно в розділу “Безпека” в пункті “Додатки” додати небезпечний IP адрес в список або повідомити про нього системному адміністратору.

Рисунок 2.4 – створення білого та чорного списку IP-адрес

Запобігання витоку даних (DLP) – це функція, яка дозволяє організаціям контролювати вміст, яким користувачі можуть ділитися в файлах за межами організації, щоб запобігти ненавмисному розкриттю конфіденційної інформації.

За допомогою DLP адміністратори можуть створювати правила, які запускають сканування файлів на наявність конфіденційного вмісту та забороняють користувачам ділитися цим вмістом. Ці правила допомагають захистити від випадкового чи навмисного обміну конфіденційними даними, такими як номери кредитних карток або ідентифікаційні номери.

Правила DLP можна застосовувати як до спільного диска, так і до кожного окремого особистого диска, надаючи організаціям детальний контроль над обміном даними. DLP допомагає організаціям підтримувати безпеку та відповідність даних, запобігаючи випадкам втрати даних.

Щоб, ввімкнути запобігання втрат даних треба у розділі «Безпека»-> «Керування доступом і даними»->«Керування DPL» та вказується список дозволених дисків та файлів які заборонено або дозволено передавати за межами організації, перш ніж вносити зміни. Інтерфейс Google дає вам змогу побачити, які файли більш важливі для забезпечення захисту від втрати інформації.

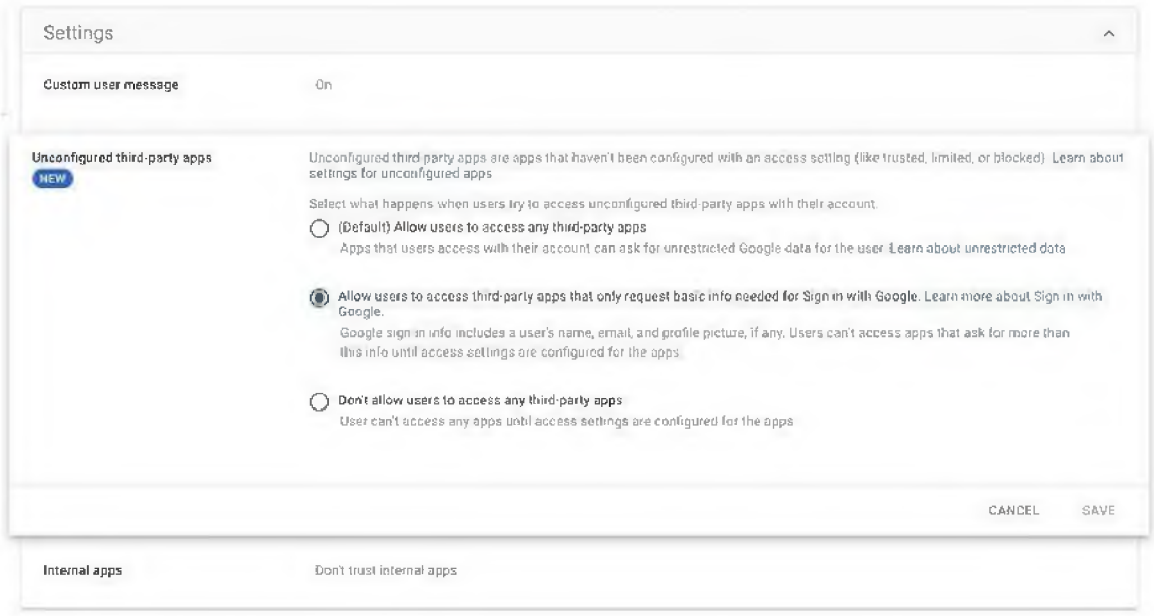

Рисунок 2.5 – запобігання витоку даних

І останній із важливих налаштувань є включення попередження про листи які неможливо автоматично перевірити. Захист Google має можливість перевіряти лише незашифровані листи, а на зашифровані не реагує, що дозволяло злочинцям передавати програми- вимагачі за допомогою стиснення файлу до формата zip. При підключенні система Google почне попереджати про підозрілі листи с файлами який неможливо автоматично перевірити, такі як шифровані або стиснені файли формату zip або rar, або про попереджати про «аномальний» тип листів- листи які є нестандартними для сфери діяльності конкретної компанії. Для підключення треба в пункті «Додатки» ввімкнути всі запропоновані налаштування безпеки.

Рисунок 2.6 – Підключення перевірки шифрованих файлів

У сучасних умовах постійних загроз, налаштування безпеки в Google

workspace набувають особливого значення. Це інструментарій, який допомагає захищати корпоративні дані та забезпечувати конфіденційність інформації. Однак, щоб максимально ефективно використовувати можливості безпеки, необхідно детально розглянути окремі аспекти налаштувань, такі як підключення двофакторної автентифікації, шифрування листів та підключення протоколів безпеки

2.1.1 Підключення двофакторної аутентифікації

Двофакторна аутентифікація (2FA) забезпечує додатковий рівень безпеки при доступі до облікових записів шляхом поєднання двох незалежних факторів аутентифікації: знання (наприклад, пароль) та володіння (наприклад, мобільний телефон). Підключення двофакторної аутентифікації забезпечує надійний захист від атак «грубою силою», підбору паролів шахраями або ж при втраті облікових даних.

При налаштуваннях, які були описані вище, двофакторна аутентифікація є обов'язковою та з'явиться при створенні аккаунта користувачем, але якщо налаштування не обране або по якимось причинам не з'явилося, то ручне підключення аутентифікації знаходиться в налаштуваннях безпеки облікового запису в підрозділі "Двоетапна перевірка".

При відкритті у користувача запросять пароль від аккаунту, який потрібен для підтвердження автентичності, а після запропонують ввести номер телефону, на який і буде відправлятись одноразовий токен для входу в систему.

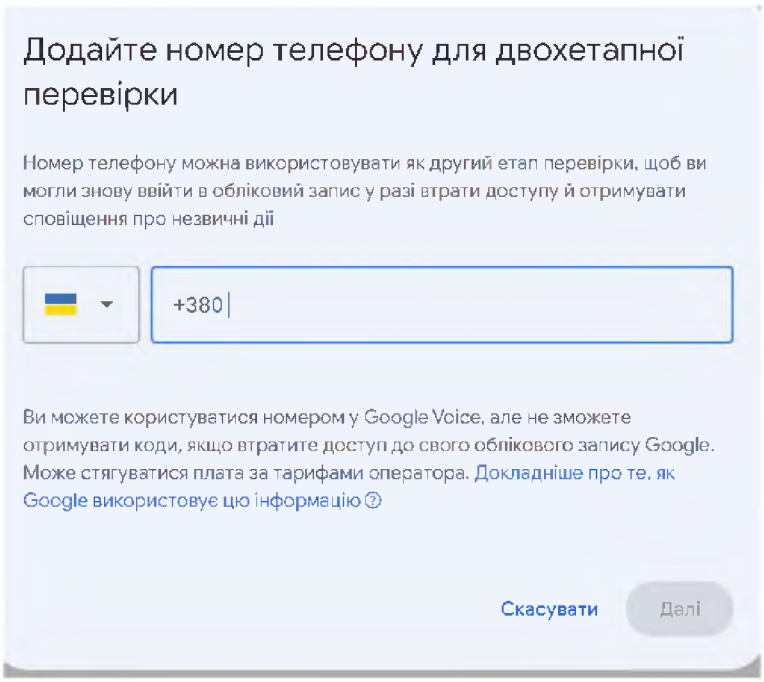

Рисунок 2.7 – Введення номеру телефону для двоетапної перевірки

Після цього користувачу на телефон в форматі СМС-повідомлення прийде число, яке треба ввести в відповідне поле. Токен є дійсним лише деякий час, тому телефон має бути в руках користувача. Сам токен є випадковим набором з 5 цифр та вказанням сайту, з якого запит був створений. Після вводу токена номер телефону стає обов'язковим етапом при входженні в обліковий запис користувача.

Система запам'ятовує пристрій з якого був зроблений вхід та не вимагає постійного проходження двофакторної автентифікації, якщо, звісно, не виставити пункт «обов'язкова автентифікація при вході» в налаштуваннях. Також система видаляє пристрій з пам'яті, якщо користувач не використовує його впродовж довгого часу. Це зроблено для безпеки при втраті пристрою та спроби входу з нього іншою людиною.

При вході користувача з іншого пристрою, або ж при спробі шахрая зайти в обліковий запис, Система запросить введення номера телефону до якого прив'язана двофакторна автентифікація та при правильному введені на нього буде відправлений одноразовий токен для входу в систему.

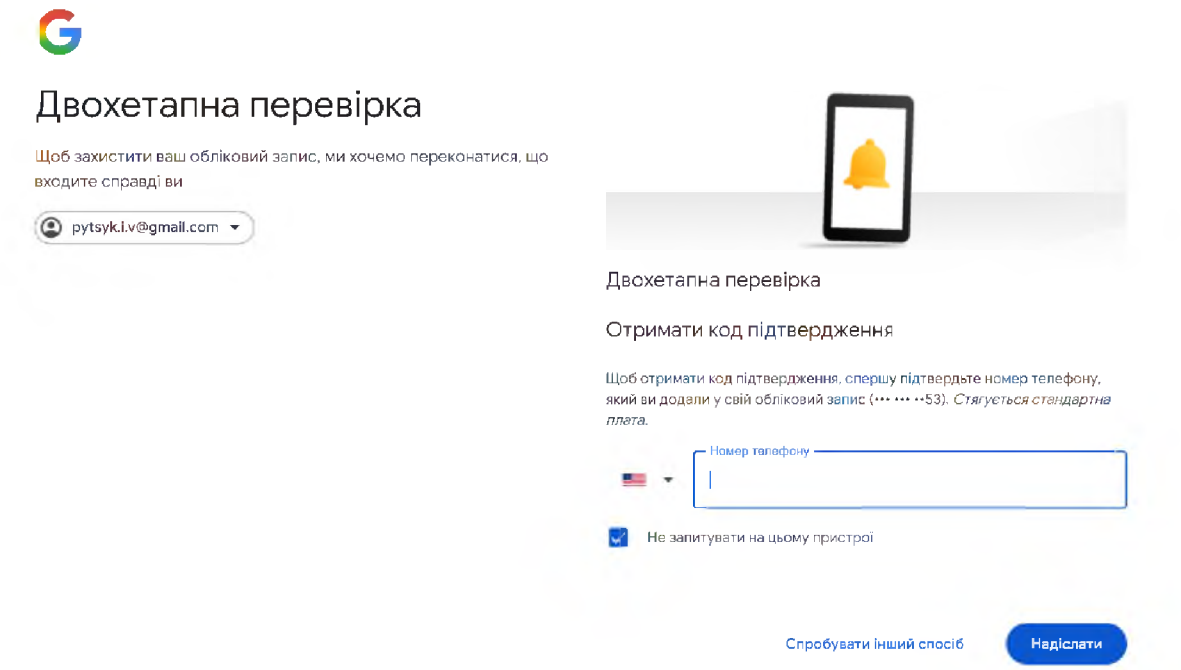

Рисунок 2.8 – Запит підтвердження номера телефону

Таким чином аккаунт користувача захищений при спробі входу в систему при кражі облікових даних, а також в купі з створенням складного паролю зменшує вірогідність взлому системи методом «грубої сили». Впровадження двофакторної автентифікації є одним із найефективніших заходів у запобіганні несанкціонованому доступу. Дослідження показують, що організації, які використовують 2FA, значно рідше стають жертвами успішних кіберзломів.

У висновку, важливість двофакторної автентифікації та складного паролю як засобів захисту облікових записів електронної пошти не може бути переоцінена. Їх інтеграція в систему безпеки є не лише рекомендованою, але й необхідною умовою для захисту конфіденційної інформації та забезпечення кібербезпеки в сучасному цифровому середовищі.

2.1.2 Шифрування даних методом E2EE

У цифровому світі, де конфіденційність і безпека даних стають все більш важливими, методи шифрування, зокрема End-to-End Encryption (E2EE), здобувають популярність як ефективний засіб захисту інформації від несанкціонованого доступу. E2EE забезпечує шифрування даних на відправнику і розшифрування на отримувачі без зберігання відкритого ключа на проміжних серверах. Цей підхід не лише забезпечує конфіденційність, але й надійність,

оскільки навіть провайдери послуг не можуть прочитати дані без ключа розшифрування.

Основні переваги E2EE включають:

1. Конфіденційність інформації: Дані шифруються на відправнику і розшифровуються лише на отримувачі. Це означає, що навіть якщо дані перехоплені під час передачі через мережу, вони залишаються безпечними.

2. Мінімізація ризиків: Інформація залишається зашифрованою на протязі всього шляху передачі, що мінімізує ризики доступу до неї третіми сторонами.

3. Довіра і конфіденційність: Використання E2EE сприяє збереженню довіри між користувачами, оскільки лише вони мають доступ до розшифрованої інформації.

Незважаючи на ці переваги, метод E2EE має деякі обмеження і недоліки, зокрема щодо передавання приватного ключа:

1. Необхідність безпечного обміну ключів: Для ефективної роботи E2EE необхідно, щоб відправник і отримувач обмінялися ключами з передачі даних. Якщо приватний ключ буде викрадено або перехоплено третьою стороною під час цього процесу, це може вразити безпеку системи.

2. Керування ключами: Керування і зберігання ключів E2EE може бути складним завданням для користувачів і розробників, оскільки це вимагає надійних систем для забезпечення їх безпеки.

Але навіть з недоліками метод шифрування End-to-End Encryption є ефективним методом шифрування даних асиметричним методом. Тому розглянемо метод шифрування листа методом E2EE.

Шифрування та дешифрування листа методом E2EE проходить в декілька етапів:

1 Спочатку створюються пара ключів RSA, один для відкритого, який використовується для шифрування та приватного, який використовується для дешифрування. Обидва ключа зберігаються в вигляді файлу з форматом PEM. Створення двох ключів для різних задач забезпечує додаткову безпеку інформації як для відправника так і для одержувача. Публічний ключ може бути відкрито

розповсюджений для шифрування даних, але лише власник приватного ключа може розшифрувати ці дані. Це усуває потребу в безпечному каналі для передачі ключа, який є вразливим місцем у симетричному шифруванні, де один ключ використовується і для шифрування, і для розшифрування.

2 Повідомлення шифрується за допомогою схеми Optimal Asymmetric Encryption Padding відкритим ключем та зберігається як зашифроване hex-повідомлення, яке рівнозначне по кількістю символів з приватним та відкритим ключем RSA.

3 Одержувач, маючи на руках шифроване hex-повідомлення та приватний ключ, розшифровує його за допомогою схеми Optimal Asymmetric Encryption Padding та отримує повідомлення відправника.

Тепер, знаючи етапи роботи End-to-End Encryption зможемо розробити код шифрування та відправлення посилання через електронну пошту. Процес шифрування починається з генерації пари ключів RSA. Це передбачає створення приватного та відповідного йому відкритого ключа, який буде використовуватись для шифрування та розшифрування посилання.

```
private_key = rsa.generate_private_key(
    public_exponent=65537,
    key_size=2048,
)
public_key = private_key.public_key()
```

Рисунок 2.9 – Створення приватного та відкритого ключа

Для збереження ключів у файловій системі використовується формат PEM. Це зручний формат для зберігання та передачі ключів. Шифрування повідомлення здійснюється за допомогою приватного ключа. Для цього використовується схема OAEP (Optimal Asymmetric Encryption Padding), яка забезпечує високий рівень безпеки.

```
message = b'This is a secret message.'

encrypted_message = public_key.encrypt(
    message,
    padding.OAEP(
        mgf=padding.MGF1(algorithm=hashes.SHA256()),
        algorithm=hashes.SHA256(),
        label=None
    )
)
```

Рисунок 2.10 – Шифрування повідомлення схемою OAEP

Для відправки зашифрованого повідомлення використовується протокол SMTP. Це забезпечує можливість передачі електронних листів через Інтернет. Для передачі інформації треба ввести адресу відправника, його пароль-додаток, який створюється в налаштуваннях безпеки, та адресу отримувача. Якщо все пройде нормально на адресу отримувача прийде зашифроване hex-повідомлення. Якщо ні- система видасть помилку.

```
sender_email = "pytsyk.i.v@gmail.com"
receiver_email = "Pitsyk.I.V@nmu.one"
password = "**** **** **** ****"

msg = MIMEMultipart()
msg['From'] = sender_email
msg['To'] = receiver_email
msg['Subject'] = "Зашифроване посилання"

msg.attach(MIMEText(encrypted_message.hex(), 'plain'))

try:
    server = smtplib.SMTP('smtp.gmail.com', 587)
    server.starttls()
    server.login(sender_email, password)
    server.sendmail(sender_email, receiver_email, msg.as_string())
    print("Лист успішно відправленний")
except Exception as e:
    print(f"Помилка: {e}")
```

Рисунок 2.11 – Відправка повідомлення з використанням SMTP сервера

При вдалому відправленні листа одержувач отримає зашифроване hex-повідомлення яке неможливо прочитати без приватного ключа. Користувачу потрібно скопіювати повідомлення в TXT файл та відкрити програму

дешифрування, яку відправник має також відіслати.

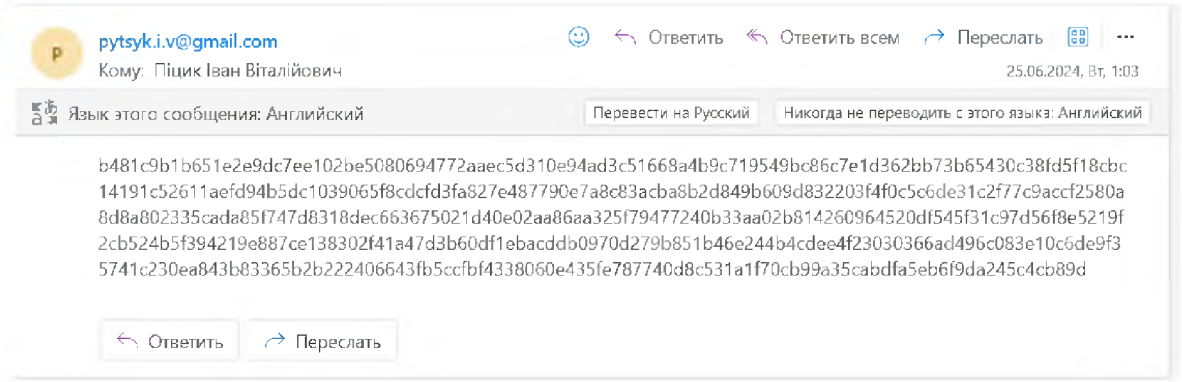

Рисунок 2.12 – отримане зашифроване повідомлення

Для початку отримувачу треба завантажити приватний ключ в форматі PEM та зашифроване посилання в форматі TXT. Програма зчитує інформацію з файлів, приватний ключ запам’ятовує, а зашифроване посилання і перетворюємо його у байтовий об'єкт з допомогою методу bytes.fromhex(), щоб мати можливість розшифрування повідомлення.

```
with open('private_key.pem', 'rb') as f:
    private_key = serialization.load_pem_private_key(
        f.read(),
        password=None,
    )
with open('Encrypted Message.txt', 'r') as f:
    encrypted_message_hex = f.read().strip()
encrypted_message = bytes.fromhex(encrypted_message_hex)
```

Рисунок 2.13 – Дешифрування повідомлення за допомогою приватного ключа

Після отримання зашифрованого повідомлення і завантаження приватного ключа використовуємо метод OAEP на об'єкт приватного ключа для розшифрування повідомлення. Ця схема забезпечує безпеку процесу шифрування і розшифрування. Отримане розшифроване повідомлення конвертується у текстовий формат і виводиться на екран.

```
decrypted_message = private_key.decrypt(
    encrypted_message,
    padding.OAEP(
        mgf=padding.MGF1(algorithm=hashes.SHA256()),
        algorithm=hashes.SHA256(),
        label=None
    )
)
print("Розшифроване посилання:\n", decrypted_message.decode('utf-8'))
```

```
Розшифроване посилання:
This is a secret message.
```

Рисунок 2.14 – Отримання дешифрованого повідомлення

2.1.3 Протоколи автентифікації електронної пошти

Довгий час електронна пошта страждала від підробки доменів компанії, що дозволяло шахраям прикидатися компаніями та оманою виманювати гроші та інформацію від користувачів. І раніше задача захисту від спуфінгу лежала на плечах користувачів тому, що у компаній не було методів підтвердження правдивості джерела, допоки не з'явились протоколи автентифікації електронної пошти.

Протоколи автентифікації електронної пошти - це процес перевірки адреси електронної пошти відправника та підтвердження того, що він уповноважений надсилати електронну пошту з певного домену. Цей процес підвищує безпеку домену, підтверджуючи серверу, що електронні листи від компанії надходять із надійного джерела. Це допомагає захистити бренд від шахрайства та підробки.

Аутентифікація допомагає запобігти шкідливим діям із використанням домену та забезпечує надійну репутацію серед інтернет-провайдерів. Вона показує, що компанія є надійним відправником і, що найголовніше, підтримує високий рівень доставки електронної пошти.

DKIM (DomainKeys Identified Mail) – це протокол, який дозволяє організації підтверджувати свою відповідальність за відправлення повідомлення шляхом підписання його таким чином, щоб поштові сервіси могли це перевірити.

Перевірка DKIM здійснюється за допомогою криптографічної автентифікації. Основною ознакою перевірки є підпис DKIM, який являє собою хеш, створений на основі різних компонентів повідомлення. Відправник використовує домен, тіло повідомлення та інші частини для створення цього підпису під час відправлення повідомлення, тому його не можна змінити пізніше.

Sender Policy Framework (SPF) - це протокол автентифікації електронної пошти, розроблений для запобігання підробці адрес відправників, що є поширеним методом у Фішингових атаках і спамі. SPF дозволяє серверу одержувача перевіряти, чи надходить вхідна електронна пошта з домену, який авторизовано адміністраторами цього домену, що робить його важливоючастиною кібербезпеки електронної пошти. Ця автентифікація корисна, оскільки у типовій Фішинговій атаці зловмисник підробляє адресу відправника, щоб вона виглядала як офіційний обліковий запис компанії або як хтось, кого жертва може знати. Запроваджуючи SPF, організації можуть захистити свій домен від зловмисників, які надсилають Фішингові або спам-листи, що покращує доступність електронної пошти та загальну репутацію.

DMARC (Domain-based Message Authentication, Reporting and Conformance), є відкритим протоколом автентифікації електронної пошти, що забезпечує захист електронної пошти на рівні домену. Він виявляє та запобігає методам підробки електронної пошти, які використовуються у Фішингових атаках, компрометації бізнес-електронної пошти (BEC) та інших видах атак, пов'язаних з електронною поштою. DMARC базується на існуючих стандартах SPF і DKIM та є першою і єдиною широко впровадженою технологією, яка робить заголовок "From" надійним.

Власники доменів можуть опублікувати запис DMARC у системі доменних імен (DNS) та визначити політику щодо обробки листів, які не пройшли автентифікацію. За допомогою DMARC власники доменів можуть чітко визначити свої методи автентифікації і встановити конкретні дії для електронних листів, які не пройшли перевірку. Цей потужний протокол допомагає боротися з численними загрозами безпеки електронної пошти.

Але, незважаючи на широке впровадження DMARC та SPF, не всі організації повною мірою використовують ці механізми або правильно налаштовують їх. Це обумовлюється складністю налаштування та перевірки коректності записів. Відсутність або неправильне налаштування записів DMARC та SPF може призвести до вразливостей, які дозволяють зловмисникам підробляти електронні листи, створюючи загрози для безпеки інформації та зниження довіри до корпоративних доменів.

Перевірка записів DMARC та SPF є важливою складовою забезпечення безпеки електронної пошти. DMARC та SPF допомагають доменам захиститися від несанкціонованого використання. Для вирішення цієї проблеми був розроблений код перевірки записів DMARC та SPF, який автоматизує процес перевірки коректності налаштувань. Такий код дозволяє швидко ідентифікувати помилки або відсутність необхідних записів, забезпечуючи надійну автентифікацію електронних листів.

Метод перевірки запису DMARC та SPF проходить в декілька етапів:

1. Спочатку системі треба отримати інформацію з доменів відправників. Для цього за допомогою створеного додатка робиться запит до платформи Gmail на отримання доменів останніх 10 листів

2. Отримана інформація з доменів передається за допомогою URL адреси до програми перевірки запису DMARC та SPF.

3. Програма зчитує інформацію з доменів та робить запит до відповідних DNS серверів, в яких зберігається інформація про відправника. Якщо домен успішно знаходиться- програма виписує всю інформацію. В ній записано основну адресу компанії, якщо адреса з якої був відправлений є дочірнім, політику безпеки DMARC, адресу на яку користувач може відправляти лист при виникненні проблеми роботи з отриманням інформації а також додатковий ідентифікатор за допомогою якого можливо перевірити те, що домен не є підробкою.

4. Отримана інформація DMARC та SPF зберігається в TXT формат для зручнішого використання та вивчення отриманої інформації

Для спрощення та автоматизації процесу створено код мовою Java Script на

платформі GoogleApps Script. Це хмарна платформа для створення та автоматизації додатків, що працюють з продуктами Google, такими Gmail. Вона дозволяє користувачам писати код для автоматизації завдань, створення користувацьких функцій та інтеграції з іншими сервісами. На ньому написано код для автоматичного отримання 10 останніх листів з пошти користувача та передачі потрібної нам інформації та створюється порожній масив emails для зберігання інформації про відправників та текстові тіла листів.

```
function doGet() {
  var threads = GmailApp.getInboxThreads(0, 10);
  var messages = GmailApp.getMessagesForThreads(threads);
  var emails = [];
```

Рис 2.15 Отримання 10 останніх листів з електронної пошти

Потім виконується два вкладених цикли для проходження по всім повідомленням:

- Зовнішній цикл проходить по масиву потоків messages.
- Внутрішній цикл проходить по масиву повідомлень у кожному потоці.

Для кожного повідомлення отримується адреса відправника.

```
for (var i = 0; i < messages.length; i++) {
  for (var j = 0; j < messages[i].length; j++) {
    var message = messages[i][j];
    var from = message.getFrom();
    emails.push({
      from: from,
    });
```

Рис 2.16 –Отримання інформації адреси та інформації відправника

Отриманий масив emails перетворюється у формат JSON, що може бути корисним для аналізу електронних листів або інтеграції з іншими системами, які підтримують формат JSON.

```
  return ContentService.createTextOutput(JSON.stringify(emails)).setMimeType
  (ContentService.MimeType.JSON);
}
```

Рисунок 2.17 – Форматування інформації в JSON

Після цього треба зберегти код та ввести його, як новий веб додаток, заради

підключення коду до нашої корпоративної пошти та отримання URL адреса на код, який потрібен для використання його в інших платформах.

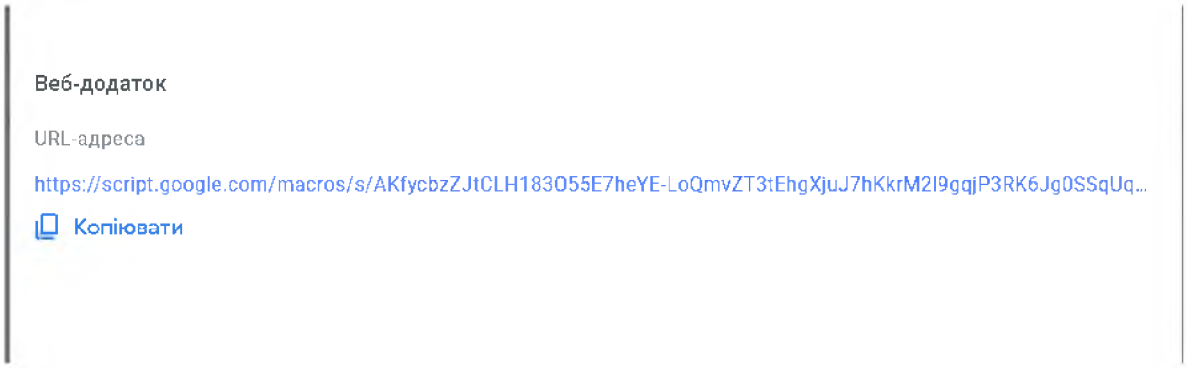

Рис 2.18 – Зберігання та отримання URL-адреси

Наступні кроки будуть проводитись на мові програмування Python, в якому розроблено методи перевірки протоколів DMARC та SPF, виділення доменів, у яких вони відсутні, та збереження інформації в TXT форматі.

Для початку вводиться script_url, який містить URL-адресу Google Apps Script, отриманий вище, до якого виконується HTTP GET запит, а потім перевіряється статус відповіді. Якщо статус 200 (OK), дані перетворюються з формату JSON у Python об'єкт. У випадку помилки при передачі інформації викликається виключення.

```
script_url = 'https://script.google.com/macros/s/AKfycbwCYpOu7_
def get_senders(script_url):
    response = requests.get(script_url)
    if response.status_code == 200:
        return response.json()
    else:
        raise Exception('Помилка при отриманні інформації')
```

Рисунок 2.19 – Підключення python до платформи Google apps script

Перед перевіркою протоколів система перевіряє правильність написання доменів. Якщо домен відправлений правильно, та з нього можливо отримати потрібну нам інформацію- він відправляється на наступні перевірки. Якщо в домені присутні неможливі формати написання, наприклад відсутність знаку «комерційна at «@»» і відсутність кінцевого домену com або ua, то з’являється помилка.

```python
def check_dmarc_spf_for_senders(script_url):
    senders = get_senders(script_url)
    results = {}
    for sender in senders:
        domain = extract_domain(sender)
        if domain:
            print(f"Перевірка домену: {domain}")
            dmarc_record = get_dmarc_record(domain)
            spf_record = get_spf_record(domain)
        else:
            print(f"Неправильний формат електронної пошти: {sender}")
```

Рисунок 2.20 – Перевірка домені на правильність форматування

Для початку формується домен для DMARC запису який виконує запит DNS типу TXT до цього домену. Якщо запис знайдено, він повертається у вигляді рядка, в якому прописано політику DMARC, основний домен компанії, якщо отриманий є субдоменом та хеш рядок, який можливо перевірити на сайтах компанії як доказ правдивості домену. Також обробляються виключення для випадків, коли запис не знайдено або домен не існує.

```python
def get_dmarc_record(domain):
    try:
        dmarc_domain = '_dmarc.' + domain
        answers = dns.resolver.resolve(dmarc_domain, 'TXT')
        return '\n'.join([rdata.to_text() for rdata in answers])
    except dns.resolver.NoAnswer:
        return ' DMARC запис не знайдено'
    except dns.resolver.NXDOMAIN:
        return 'DMARC домен не існує'
```

Рисунок 2.21 – Перевірка DNS серверів протоколу DMARC

Потім формується запит до іншого DNS в якому зберігається інформація про SPF протокол. Якщо при перевірці всіх TXT записів на наявність SPF запису система отримає “v=spf1”- значить домен є довіреним. Якщо ні, або неможливо знайти інформацію про домен в DNS- з’являється повідомлення с попередженням.

```
def get_spf_record(domain):
    try:
        answers = dns.resolver.resolve(domain, 'TXT')
        for rdata in answers:
            if 'v=spf1' in rdata.to_text():
                return rdata.to_text()
        return 'запис SPF не знайдено'
    except dns.resolver.NoAnswer:
        return 'запис SPF не знайдено'
    except dns.resolver.NXDOMAIN:
        return 'SPF домен не існує'
```

Рисунок 2.22 – Перевірка DNS серверів протоколу SPF

Коли вся інформація буде оброблена- вона зберігається в TXT файл та відправляється користувачу або системному адміністратору.

```
results = check_dmarc_spf_for_senders(script_url)
for domain, records in results.items():
    print(f"Domain: {domain}")
    print(f"DMARC: {records['dmarc']}")
    print(f"SPF: {records['spf']}")
    print("\n")
```

Рисунок 2.23 – Збереження інформації в TXT файл

В файлі зберігається інформація про домен, протоколи DMARC та SPF, а при відсутності одного з них висвічується повідомлення про можливу небезпеку заданого домену. Таким чином можна швидко отримувати потрібну нам інформацію та мати більшу довіру до доменів, у який підключенні всі необхідні протоколи безпеки.

```
Domain: promo.epicentrk.ua
DMARC: "v=DMARC1; p=none"
SPF: "v=spf1 include:spf2.esputnik.com ~all"

Domain: mxtoolbox.com
DMARC: "v=DMARC1; p=reject; rua=mailto:634990a7@mxtoolbox.dmarc-report.com,mailto:
SPF: "v=spf1 redirect=mxtoolbox.com.hosted.spf-report.com"

Domain: google.com
DMARC: "v=DMARC1; p=reject; rua=mailto:mailauth-reports@google.com"
SPF: "v=spf1 include:_spf.google.com ~all"

Domain: accounts.google.com
DMARC: "v=DMARC1; p=reject; rua=mailto:mailauth-reports@google.com"
SPF: "v=spf1 redirect=_spf.google.com"

Domain: send.tickets.ua
DMARC: DMARC domain does not exist
SPF: "v=spf1 include:spf2.esputnik.com ~all"
Небезпечний домен, можливий фішинг
```

Рисунок 2.24 – Отримана інформація в форматі TXT

Таким чином отримується інформація DMARC і SPF та на її основі користувач може вирішити чи може він мати довіру до сайту, у якого відсутні всі потрібні протоколи безпеки, а також переконатися в безпеці сайту, у якого все присутнє. Перевірка протоколів безпеки є важливим етапом формуванні довіри до електронної пошти та боротьби с підробкою доменів компанії.

2.1.4 Аналіз вкладень на наявність шкідливого програмного забезпечення

Вкладення в електронній пошті – це файли, які додаються до електронних листів для передачі різноманітної інформації. Вкладення можуть містити документи, зображення, відео, аудіофайли та інші типи файлів. Вони роблять електронні листи зручними для передачі великих обсягів інформації, які не можуть бути вміщені безпосередньо в текст листа.

Зловмисники використовують вкладення в електронній пошті для поширення шкідливого програмного забезпечення різними методами. Вони можуть вкладати файли з шкідливим кодом у документи Word або Excel з макросами, PDF файли, архіви (наприклад, ZIP або RAR), виконувані файли (.exe) або навіть мультимедійні файли, які при відкритті запускають шкідливий код і заражають комп'ютер. Використовуючи методи соціальної інженерії,

зловмисники часто маскують свої повідомлення під легітимні листи від відомих організацій чи осіб, щоб обдурити користувача і змусити його відкрити вкладення.

Тому користувачу важливо мати під рукою засоби перевірки програмного забезпечення, при чому бажано це робити до встановлення файлу на персональний комп'ютер. Для таких речей існує онлайн API сервіс VirusTotal. Він, використовуючи базу даних шкідливих вкладень, численних антивірусних програм та віртуальних середовищ сканує отриманий файл та видає інформацію про безпеку або небезпеку програмного забезпечення.

VirusTotal – це онлайн-сервіс, який дозволяє перевіряти файли та URL-адреси на наявність шкідливого програмного забезпечення, використовуючи бази даних численних антивірусних програм. Сервіс об'єднує результати з понад 70 різних антивірусних рішень і інструментів для аналізу шкідливого програмного забезпечення, що значно підвищує точність і надійність виявлення загроз.

VirusTotal є ефективним інструментом для виявлення та аналізу шкідливого програмного забезпечення. Завдяки використанню численних антивірусних механізмів та можливостям аналізу поведінки файлів, VirusTotal надає користувачам потужні інструменти для забезпечення кібербезпеки. Інтеграція через API дозволяє автоматизувати процеси сканування та отримання звітів, що робить цей сервіс надзвичайно корисним для фахівців з безпеки.

Але встановлювати файл, потім пересилати його на сайт VirusTotal щоб лише потім отримати звіт безпеки може бути не лише довго, а й небезпечно тому, що велика кількість шкідливих програмних забезпечень можуть почати спрацьовувати відразу при потраплянні в персональний комп'ютер.

Тому заради спрощення процесу та підвищення безпеки був розроблений метод знаходження, сканування, та створення звіту вкладень електронної пошти. Метод отримання та сканування проходить в декілька етапів:

1. Спочатку системі треба підключитись до облікового запису користувача. Після підключення вона зчитує всі листи, які знаходяться в папці вхідні та записує ті, у який присутні файли вкладення.

2. Після запису вона відправляє їх на сервери VirusTotal та робить запит на перевірку файлів. Після сканування сервери відправляють звіт назад в систему користувача.

3. Отриманий звіт зберігається в TXT форматі, в якому записані назви антивірусів та те, чи знайшли вони небезпеку у вкладеному файлі.

Тепер більш детально розглянемо методи забезпечення захисту від шкідливих вкладень. Для початку потрібно ввести всю необхідну інформацію: пароль додатку, який потрібно створити в налаштуваннях безпеки, електрону пошту, Imap сервер Googleта ключ API який знаходиться на аккаунті користувача Virus Total. Пароль додатку є унікальним та його треба створювати окремо від звичайного пароля від облікового запису. Він використання облікового запису в сторонніх програмних забезпеченнях без використання основного пароля облікового запису.

```
IMAP_SERVER = "imap.gmail.com"
EMAIL_ACCOUNT = "pytsyk.i.v@gmail.com"
PASSWORD = "**** **** **** ****"
API_KEY = '572d16fe6c372fbe3eb7f518...'
```

Рисунок 2.25 підключення обліково запису користувача

Після введення необхідної інформації встановлюється з'єднання з поштовим сервером Googleта виконується авторизація за допомогою електронної адреси та пароля. З'єднання встановлюється через криптографічний протокол SSL заради забезпечення безпеки при підключенні до серверів.

```
def connect_to_mail():
    mail = imaplib.IMAP4_SSL(IMAP_SERVER)
    mail.login(EMAIL_ACCOUNT, PASSWORD)
    return mail
```

Рисунок 2.6 – запит з'єднання з серверами Google

Далі система підключається до папки електронної пошти «Вхідні» та виконує пошук листів у вибраній папці заради збереження ідентифікаторів отриманих повідомлень.

```
def fetch_attachments(mail):
    mail.select('inbox')
    result, data = mail.search(None, 'ALL')
    mail_ids = data[0].split()
    attachments = []
```

Рисунок 2.27 –Підключення системи до папки електронної пошти

Кожне збережене повідомлення перетворюється в зрозумілий для програми форматі бітів. Після форматування перевіряється інформація кожного повідомлення. Якщо частиною листа є вкладення- лист запам'ятовується, якщо ні-лист пропускається. Дані файлів декодуються та додаються в список для подальших обробок.

```
for mail_id in mail_ids:
    result, msg_data = mail.fetch(mail_id, '(RFC822)')
    raw_email = msg_data[0][1]
    msg = email.message_from_bytes(raw_email)

    for part in msg.walk():
        if part.get_content_maintype() == 'multipart':
            continue
        if part.get('Content-Disposition') is None:
            continue
        file_name = part.get_filename()
        if bool(file_name):
            attachments.append((file_name, part.get_payload(decode=True)))
```

Рисунок 2.28 – Пошук вкладень в листах електронної пошти

Після декодування кожен з вкладень перевіряється через API Virustotal. Файл сканують на отримання інформації імені файлу та його вміст, після чого робиться Здійснюється POST-запит до API VirusTotal, надсилаючи файл для

сканування. Користувач завантажує файл на сервер VirusTotal через веб-інтерфейс або за допомогою API. Файл передається різним антивірусним механізмам для аналізу.

VirusTotal використовує понад 70 антивірусних механізмів від різних постачальників безпеки. Кожен антивірусний механізм запускає власні алгоритми для перевірки файлу на наявність шкідливого програмного забезпечення. Кожен антивірусний механізм повертає результат сканування, який містить інформацію про те, чи було виявлено шкідливий код у файлі. Результати включають назву загрози (якщо така виявлена), тип загрози (вірус, троян, хробак тощо) та рівень небезпеки. Отриманий результат зберігається в формат TXT

```
def scan_attachment(file_content, file_name, api_key):
    url = 'https://www.virustotal.com/vtapi/v2/file/scan'
    files = {'file': (file_name, file_content)}
    params = {'apikey': api_key}
    response = requests.post(url, files=files, params=params)
    return response.json()
def save_scan_result(file_name, result):
    with open("scan_results.txt", "a") as file:
        file.write(f"Scanned {file_name}: {result}\n")
```

Рисунок 2.29 – сканування вкладень за допомогою API VirusTotal

Для перевірки працездатності програми було передано безпечний файл за допомогою електронної пошти. Відправник прикріплює файл та відправляє його на пошту, на яку встановлений захист. Після запуску програми отримано TXT файл в якому при перевірці 70 антивірусними програмами лише один порахував файл як небезпечний, що можна скинути на помилку антивірусної програми, а отже файл вважається безпечним .

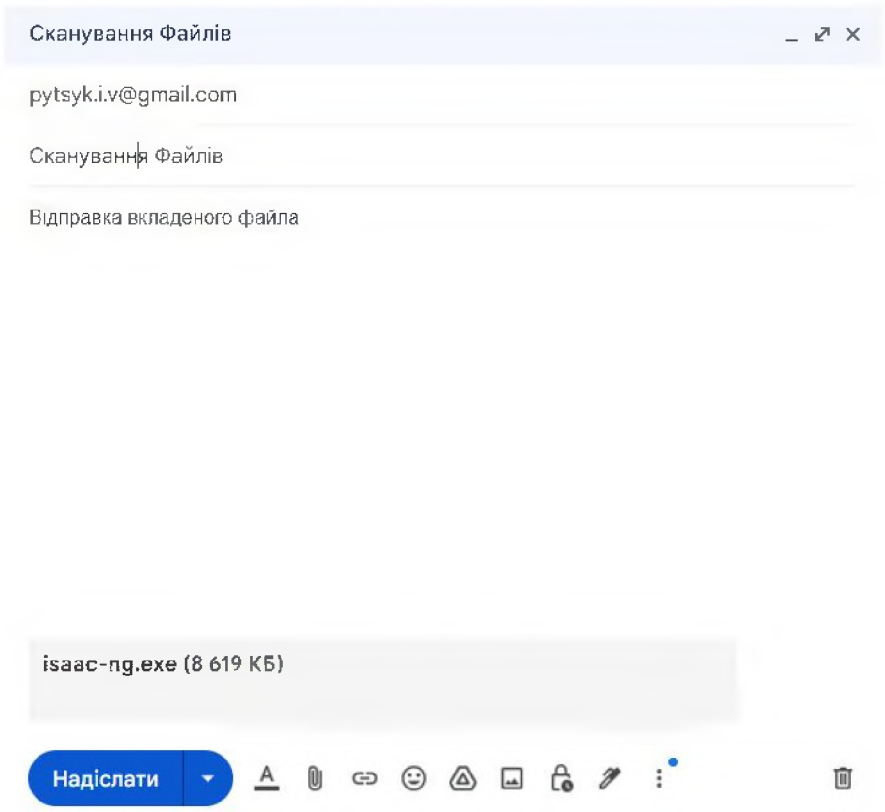

Рисунок 2.30 – Відправлення вкладення до користувача

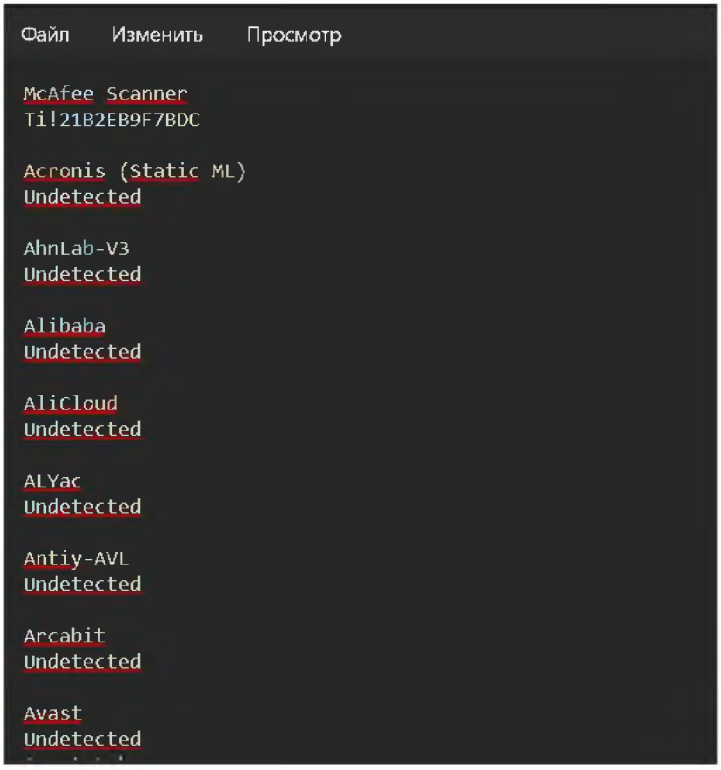

Рисунок 2.31 – Отриманий звіт сканування VirusTotal

Таким чином застосовано метод сканування та захисту системи електронної

пошти від вкладень шкідливого програмного забезпечення. Але треба пам'ятати, що ні один метод не є на сто відсотків безпечним, тому користувачу треба бути пильним та не встановлювати програмне забезпечення без початкової перевірки відправника, навіть якщо програма видала звіт безпеки вкладеного файлу.

2.1.5 Підвищення освічення персоналу

Для організацій існує небагато інвестицій, які принесуть більший прибуток, ніж реалізація програми навчання кібербезпеки для своїх співробітників. З точки зору кібербезпеки, співробітники є найбільшим активом вашої організації та вашою найбільшою відповідальністю.

Добре навчений, обізнаний співробітник може діяти на упередження виявляючи перші ознаки атаки та сповіщаючи свою команду кібербезпеки про небезпеку. З іншого боку, ненавчені працівники можуть мимоволі потрапити в пастки, які можуть коштувати їхнім організаціям мільйони доларів.

Одна ключова відмінність між цими двома працівниками? Навчання з кібербезпеки. Навчання з питань кібербезпеки навчає співробітників тому, як виявляти загрози кібербезпеці та реагувати на них. Навчання охоплює різноманітні теми, зокрема такі сфери, як захист даних, керування паролями та безпека електронної пошти.

Навчання часто проводиться за кількома модулями та містить тести, щоб співробітники зрозуміли матеріал. Організації часто проводять симуляції Фішингу до та після навчання, щоб визначити контрольні показники, виміряти покращення та визначити співробітників, які потребують подальшого навчання.

Навчання з кібербезпеки можна проводити особисто, онлайн у режимі реального часу або асинхронно з використанням записаних матеріалів.

Співробітники навчаються виявляти поширені атаки, такі як шахрайство соціальної інженерії, і навчать використовувати технології кібербезпеки, такі як менеджери паролів або VPN. Кожна організація, незалежно від того, велика чи мала, є вразливою до кібератак, і інвестиції в навчання з питань кібербезпеки є значним кроком до зменшення ймовірності того, що бізнес стане жертвою атаки.

Коли компанія розробляє навчальні курси по кібербезпеці вона оцінює

загальну безпеку яка вже є та виділяє найслабші місця, наприклад чи є безпечні передавання документів через листи, чи є прогалини в міжофісних електронних листа і тому подібне. Коли найслабша ланка виявлена компанія робить на неї зосередження при розробці курсу.

Також важливо дізнатися чи знають працівники базову інформацію по кібербезпеці. Для такого треба провести оцінювання обізнаності співробітників, щоб не витрачати час працівників на інформацію яку вони вже і так знають.

Важливо, щоб компанія робила навчання індивідуальним, тому що є велика вірогідність того, що якісь співробітники вже ставали жертвами крадіжки даних, аотже треба заохочувати їх ділитися досвідом, залучаючи їх також до захисту компанії

Деякі компанії також можуть створювати імітацію кібератак для кожного відділу вашої компанії. Ці навчальні тренування з «живою стрільбою» можуть покращити знання кібербезпеки та підготувати всіх, якщо настане час, коли це не просто навчання.

Також важливо зробити акцент навчання нових співробітників, що є основною мішенню для зловмисників. Вони не знають, як працюють системи організації, не знають, до кого звернутися за допомогою, і тому вразливі до соціальної інженерії та Фішингу. Щоб боротися з цим, компанії включають навчання з кібербезпеки як частину процесу адаптації нового найму, який не лише охоплює технічний вміст, а вживає заходів, щоб переконатися, що нові співробітники розуміють важливість кібербезпеки, сприймають свою роль і розуміють, як ділитися будь-якими попереджувальними ознаками атак. Створення культури, яка наголошує на обміні інформацією та уникає звинувачення окремих осіб, допомагаєгарантувати, що нові співробітники прийдуть до IT-команди, якщо вони зіткнуться з будь-якими підозрілими ситуаціями.

Вартість навчання співробітників з кібербезпеки може значно варіюватися в залежності від методів, тривалості та глибини навчальних програм. Методи навчання можуть відрізняти від компанії до компанії, в залежності від їх бюджету,розміру, важливості безпеки та тому подібного.

Існують безкоштовні ресурси, деякі базові тренінги можна знайти безкоштовнона таких платформах, як YouTube або спеціалізовані веб-сайти з кібербезпеки. Однак якість і глибина таких курсів можуть бутинеоднорідними.

Для більш точного але все ще бюджетного варіанту багато провайдерів пропонують онлайн-курси з кібербезпеки, які можуть коштувати від $50 до

$500 за курс. Наприклад, популярні платформи, такі як Coursera та Udemy, пропонують курси в цьому ціновому діапазоні.

Якщо компанія веде крупний бізнес в сфері, яка часто піддається нападу, потрібно починати вводити поглиблені програми, такі як сертифікаційні курси (наприклад, Certified Information Systems Security Professional - CISSP), можуть коштувати від $1000 до $5000 і більше, залежно від провайдера та тривалості курсу. Вони проводять організація внутрішніх тренінгів з залученням зовнішніх експертів або проведення симуляцій кібернападів.

Але важливо щоб компанії не розглядали ціну за курси як збитки, а вважали ці витрати як інвестицію у захист компанії від потенційних кібератак та витоку даних, що може призвести до набагато більших фінансових втрат у разі успішного нападу.

Таким чином, навчання співробітників навіть базовими курсами знижує ймовірність втрати даних через людський фактор. Чим більший відсоток працівників добре підготовлені та чим глибше вони володіють знаннями з кібербезпеки, тим менше ризик, що компанія зазнає значних збитків від кібератак. Результати цього дослідження свідчать про те, що інвестиції в навчання персоналу є критично важливими для зміцнення кібербезпекових позицій організації. Систематичний підхід до підвищення кваліфікації працівників сприяє створенню стійкої та захищеної інформаційної інфраструктури, що є ключовим фактором у забезпеченні безперервності бізнес-процесів та збереженні репутації компанії.

Крім того, постійне навчання сприяє формуванню культури безпеки в організації, де кожен співробітник усвідомлює свою роль у захисті даних та активно сприяє мінімізації ризиків. Регулярні тренінги та оновлення знань

забезпечують працівникам навички, необхідні для своєчасного розпізнавання та реагування на потенційні загрози. Це, в свою чергу, дозволяє швидко адаптуватися до нових викликів та зменшує ймовірність успішних кібератак.

Таким чином, ефективне навчання та підвищення кваліфікації персоналу є невід'ємною частиною стратегії кібербезпеки будь-якої організації. Інвестиції в освітні програми для співробітників не лише підвищують рівень безпеки, але й сприяють загальному розвитку компанії, конкурентоспроможність на ринку.

Висновок до другого розділу

У другому розділі здійснено аналіз методів захисту корпоративної пошти на платформі Google workspace . Детально розглянуто різноманітні інструменти та налаштування безпеки, доступні в цій платформі. Підключення двофакторної автентифікації було визначено як ключовий метод захисту облікових записів, що значно знижує ризик несанкціонованого доступу.

Було розроблено програму шифрування інформації методом End-to-End Encryption та відправки зашифрованого повідомлення на пошту одержувача. Також був застосований автоматичної перевірки записів DMARC та SPF доменів електронних листів, які знаходяться в папці «Вхідні», що є важливою складовою забезпечення безпеки.

Особливу увагу приділено навчанню співробітників основам кібербезпеки, що є критично важливим для підтримання високого рівня захисту корпоративної пошти, зменшення вірогідності втрати інформації та забезпечення загальної безпеки і дотримання нормативних вимог щодо захисту даних.

РОЗДІЛ 3. ЕКОНОМІЧНА ЧАСТИНА

Метою виконання економічного розділу є техніко-економічне обґрунтування доцільності запровадження запропонованих рішень для захисту корпоративної пошти на платформі Gmail. Основними задачами є визначення економічної ефективності впровадження методів захисту, оцінка витрат та аналіз економічної вигоди для організації

3.1 Розрахунок (фіксованих) капітальних витрат

Нормування праці в процесі розробки політики безпеки інформації істотно ускладнено через творчій характер праці спеціалістів з інформаційної безпеки. Проте трудомісткість розробки політики безпеки інформації може бути розрахована на основі трудомісткості робіт, які виконуються.

Трудомісткість розробки політики безпеки інформації визначається тривалістю кожної робочої операції, починаючи з складання технічного завдання і закінчуючи оформленням документації (за умови роботи одного спеціаліста з інформаційної безпеки):

$$t = t_{тз} + t_{в} + t_{а} + t_{взз} + t_{озб} + t_{овр} + t_{д}, \qquad (3.1)$$

$t_{тз}$ – тривалість складання технічного завдання на розробку політики безпеки інформації;

$t_{в}$ – тривалість розробки концепції безпеки інформації у організації;

$t_{а}$ – тривалість процесу аналізу ризиків;

$t_{взз}$ – тривалість визначення вимог до заходів, методів та засобів захисту;

$t_{озб}$ – тривалість вибору основних рішень з забезпечення безпеки інформації;

$t_{овр}$– тривалість організації виконання відновлювальних робіт і забезпечення неперервного функціонування організації;

$t_{д}$ – тривалість документального оформлення політики безпеки.

Таблиця 3.1 – Часові показники трудомісткості розробки ПБ

Показник	Кількість годин
tтз	13
tв	6
ta	2
tвз	5
tозб	4
tовр	14
tд	4

За формулою 3.1 трудомісткість розробки ПБ становить:

$$t= 13+6+2+5+4+14+4,$$

t=48 годин

Витрати на розробку ПБ являються сумою витрат на заробітну плату спеціаліста і вартості витрат машинного часу, необхідного для розробки ПБ.

Розраховуються за формулою 3.2:

$$Крп = Ззп + Змч \quad (3.2)$$

де Крп - витрати на розробку політики безпеки інформації; Ззп - заробітна плата спеціаліста з інформаційної безпеки;

Змч – вартість витрат машинного часу, необхідного для розробки ПБ;

Заробітна плата виконавця враховує основну і додаткову заробітну плату, а також відрахування на соціальне потреби (пенсійне страхування, страхування на випадок безробіття, соціальне страхування тощо) и визначається за формулою:

$$Ззп= t \cdot Зпр \text{ , грн,} \quad (3.3)$$

де t – загальна тривалість створення ПЗ, годин;

Зпр – середньогодинна заробітна плата системного адміністратора нарахуваннями, грн/годину.

$$Ззп= 48 \cdot 145$$

Ззп=5232

Вартість машинного часу для розробки політики безпеки інформації на ПК визначається за формулою:

$$З_{мч} = t \cdot С_{мч} \ , \ \text{грн}, \tag{3.4}$$

де t – трудомісткість розробки політики безпеки інформації на ПК,годин;

*С*мч – вартість 1 години машинного часу ПК, грн./година.

Для отримання вартості 1 машинного часу треба скористатися формулою:

$$\text{Смч} = \text{Р} \cdot \text{Се} + \frac{\text{Фзал} \cdot \text{На}}{Fp} + \frac{\text{Клпз} \cdot \text{Напз}}{Fp} \tag{3.5}$$

де Р – встановлена потужність ПК, кВт (Р= 0,18 кВт);

Се– тариф на електричну енергію, грн/кВт·година(Се=1,68грн/кВт·година);

Фзал – залишкова вартість ПК на поточний рік, грн(Фзал = 5000 грн).; На – річна норма амортизації на ПК, частки одиниці (1/3 на рік);

Напз – річна норма амортизації на ліцензійне програмне забезпечення, частки одиниці (100% на рік);

Клпз – вартість ліцензійного програмного забезпечення, грн (2030 грн);

Fр – річний фонд робочого часу (за 40-годинного робочого тижня Fр = 1920.)

$$\text{Смч} = 0{,}18 \cdot 1{,}68 \frac{5000 \cdot 1/3}{1920} + \frac{2030 \cdot 1}{1920}$$

$$\text{Смч} = 0{,}3024 + \frac{125}{144} + \frac{203}{192}$$

$$\text{Смч} = \frac{189}{625} + \frac{125}{144} + \frac{203}{192}$$

Смч=2,22

Тепер маючі дані рахуємо по формулі 3.4:

$$\text{Змч} = 48 \cdot 2{,}22$$

$$\text{Змч} \approx 107$$

Тепер можемо розрахувати витрати на розробку політики безпекиінформації за формулою 3.2:

Крп =5232+107

Крп= 5339

Капітальні (фіксовані) витрати на проектування та впровадження проектного варіанта системи інформаційної безпеки складають:

$$К = Кпр + Кзпз + Крп + Кпз + Кнавч + Кн, \text{ грн} \quad (3.6)$$

де Кпр – вартість розробки проекту інформаційної безпеки та залучення для цього зовнішніх консультантів, (Крп=5232)

Кзпз –вартість закупівель ліцензійного основного й додаткового програмного забезпечення (ПЗ), (Кзпз=10145);

Крп – вартість розробки політики безпеки інформації, (Крп=5339);

Кнавч – витрати на навчання технічних фахівців і обслуговуючого персоналу,. Для малого підприємства навчання дорівнює 500 грн за одного фахівця;

Кн –витрати на встановлення обладнання та налагодження системи інформаційної безпеки, тис. грн. Так як для створення корпоративної пошти не потрібно докупляти додаткове встановлення обладнання та налагодження системи, то він дорівнює 0;

За формулою 3.6:

К= 5232+10145+5339+500 = 21216 грн

3.2 Розрахунок поточних (експлуатаційних) витрат

Експлуатаційні витрати – це поточні витрати на експлуатацію та обслуговування об'єкта проектування за визначений період (наприклад, рік), що виражені у грошовій формі.

Річні поточні (експлуатаційні) витрати на функціонування системи інформаційної безпеки складають:

$$С = С_в + С_к + С_{ак}, \text{ тис. грн.} \quad (3.7)$$

Де $С_в$- вартість Upgrade-відновлення й модернізації системи ;

$С_к$ - витрати на керування системою в цілому ;

$С_{ак}$-витрати, викликані активністю користувачі системи інформаційної безпеки.

Витрати на керування системою в цілому ($С_к$) вираховується за формулою:

$$С_к = С_н + С_а + С_з + С_{св} + С_{ел} + С_о + С_{тос}, \text{ грн.} \quad (3.8)$$

Де $С_н$- Витрати на навчання адміністративного персоналу й кінцевих користувачів ($С_н$=0).

$С_а$- Річний фонд амортизаційних відрахувань вираховуються заформулою:

$$С_а = К_{зпз} * А \quad (3.9)$$

Єдине на що треба робити амортизаційні відрахування це на покупку ліцензійного програмного забезпечення та домену, через це отримаємо, що річний відсоток амортизації на 2 роки використання буде:

$$А = \frac{100}{2} \% = 50\%$$

$К_{зпз}$ = 10145 грн

Отже використовуючи формулу 3.9 ми отримуємо:

$$С_а = 10145 \cdot 50\% = 5072 \text{ грн}$$

Сз- Річний фонд заробітної плати інженерно-технічного персоналу, що обслуговує систему інформаційної безпеки складає:

$$С_з = З_{осн} + З_{дод}, \text{ грн} \quad (3.10)$$

де $З_{осн}$, $З_{дод}$ - основна і додаткова заробітна плата відповідно, грн на рік.

$З_{осн}$ = 13 276 грн на місяць

$З_{дод}$ вираховується в розмірі 8-10% від основної заробітної плати.

$$С_з = 13276 \cdot 12 + (13276 \cdot 12 \cdot 0{,}08)$$

$$С_з = 159312 + 12744$$

$$С_з = 172056 \text{ грн на рік}$$

Для платників податків на спрощений системі ставка ЄСВ становить 22%, отже:

$$С_{св} = 307243 \cdot 0,22$$

$$С_{св} = 67593$$

Вартість електроенергії, що споживається апаратурою системою інформаційної безпеки протягом року визначається за формулою:

$$С_{ел} = Р \cdot F_р \cdot Ц_е \text{ , грн,} \qquad (3.11)$$

де Р – встановлена потужність апаратури інформаційної безпеки, кВт (Р= 1 Квт);

$F_р$ – річний фонд робочого часу системи інформаційної безпеки($F_р$ = 1920);

$Ц_е$ – тариф на електроенергію, грн/кВт·годин ($Ц_е$ = 4,32 грн/кВт·год)

$$С_{ел} = 1 \cdot 1920 \cdot 4,32 = 8294 \text{ грн}$$

Витрати на залучення сторонніх організацій для виконання деяких видів обслуговування, навчання та сертифікацію обслуговуючого персоналу ($С_о$) визначаються за даними організації ($С_о$= 1000)

$С_{тос}$- Витрати на технічне й організаційне адміністрування та сервіс системи інформаційної безпеки вираховуються за формулою:

$$С_{тос} = К \cdot 0,1$$

$$С_{тос} = 13101 \cdot 0,1$$

$$С_{тос} = 1310$$

Отримавши всі дані можливо порахувати витрати на керування системою в цілому за формулою 3.8:

$$С_к = 0 + 5072 + 172056 + 8294 + 1000 + 1310$$

$$С_к = 187732$$

$С_{ак}$ - витрати, викликані активністю користувачів системи інформаційної безпеки ($С_{ак}$=1000).

За формулою 3.7 річні поточні витрати на функціонування системи інформаційної безпеки:

$$С = 0 + 187732 + 1000 = 188732$$

3.1.1 оцінка можливого збитку від атаки (злому)

Необхідні *вихідні дані* для розрахунку:

$t_п$ – час простою вузла або сегмента корпоративної мережі внаслідокатаки,

годин($t_п = 8$);

$t_в$ – час відновлення після атаки персоналом, що обслуговує корпоративну мережу, годин ($t_в = 3$);

$t_{ви}$ – час повторного введення загубленої інформації співробітниками атакованого вузла або сегмента корпоративної мережі, годин($t_{ви} = 1$);

$З_о$ – заробітна плата обслуговуючого персоналу (адміністраторів та ін.), грн на місяць($З_о = 23276$);

$З_с$ – заробітна плата співробітників атакованого вузла або сегмента корпоративної мережі, грн на місяць($З_с = 26000$);

$Ч_о$ – чисельність обслуговуючого персоналу (адміністраторів та ін.), осіб.($Ч_о = 1$);

$Ч_с$ – чисельність співробітників атакованого вузла або сегмента корпоративної мережі, осіб. ($Ч_с = 20$);

О – обсяг продажів атакованого вузла або сегмента корпоративної мережі, грн у рік (О = 1000000);

$П_{зч}$ – вартість заміни встаткування або запасних частин, грн ($П_{зч}$ = 5450);

I – число атакованих вузлів або сегментів корпоративної мережі(I = 2);

N – середнє число атак на рік (N = 5).

Упущена вигода від простою атакованого вузла або сегмента корпоративної мережі становить:

$$U = П_п + П_в + V, \quad (3.12)$$

Де $П_п$ – оплачувані втрати робочого часу та простої співробітників атакованого вузла або сегмента корпоративної мережі, грн;

$П_в$ – вартість відновлення працездатності вузла або сегмента корпоративної мережі (переустановлення системи, зміна конфігурації та ін.), грн;

V – втрати від зниження обсягу продажів за час простою атакованого вузла або сегмента корпоративної мережі, грн.

Втрати від зниження продуктивності співробітників атакованого вузла або сегмента корпоративної мережі являють собою втрати їхньої заробітної плати

(оплата непродуктивної праці) за час простою внаслідок атаки:

$$П_п=\frac{\sum Зс}{F}\cdot t_п \quad \text{—} \tag{3.13}$$

де F- місячний фонд робочого часу (при 40-а годинному робочому тижні становить 176 ч).

Витрати на відновлення працездатності вузла або сегмента корпоративної мережі включають кілька складових:

$$П_в = П_{ви} + П_{пв} + П_{зч} \tag{3.14}$$

де $П_{ви}$ – витрати на повторне уведення інформації, грн;

$П_{пв}$ – витрати на відновлення вузла або сегмента корпоративноїмережі, грн;

$П_{зч}$ – вартість заміни устаткування або запасних частин, грн .

Втрати від зниження продуктивності співробітників атакованого вузла або сегмента корпоративної мережі являють собою втрати їхньої заробітної плати (оплата непродуктивної праці) за час простою внаслідок атаки:

$$П_{ви} = \frac{\sum Зс}{F} \cdot t_{ви}$$

$$Пви = \frac{26000 \cdot 25}{176} \cdot 1$$

$$Пви = 3693$$

Витрати на відновлення вузла або сегмента корпоративної мережі визначаються часом відновлення після атаки і розміром середньогодинної заробітної плати обслуговуючого персоналу (адміністраторів):

$$П_{пв} = \frac{\sum Зс}{F} \cdot t_{пв}$$

$$П_{пв} = \frac{23276 \cdot 25}{176} \cdot 3$$

$$П_{пв} = 9918$$

Тепер за формулою 3.14:

$$П_в = 3693 + 9918 + 5450$$

$$П_в = 13611$$

Втрати від зниження очікуваного обсягу продажів за час простою

атакованого вузла або сегмента корпоративної мережі визначаються виходячи із середньогодинного обсягу продажів і сумарного часу простою атакованого вузла або сегмента корпоративної мережі:

$$V=\frac{O}{Fг} \cdot (t_п + t_в + t_{ви})$$

де $F_г$ – річний фонд часу роботи організації (52 робочих тижні, 5-ти денний робочий тиждень, 8-ми годинний робочий день) становить близько 2080 ч.

$$V=\frac{1000000}{2080} \cdot (8+3+1)$$

$$V= 5769$$

За формулою 3.12:

$$U = 29545 + 13611 + 5769 = 48925$$

Таким чином, загальний збиток від атаки на вузол або сегмент корпоративної мережі організації складе:

$$B=\sum_i\sum_n U \qquad (3.18)$$

$$B = 5 \cdot 2 \cdot 48925 = 489250$$

3.3 Загальний ефект від впровадження системи інформаційної безпеки

Загальний ефект від впровадження системи інформаційної безпеки визначається з урахуванням ризиків порушення інформаційної безпеки і становить:

$$E = B \cdot R – C \qquad (3.19)$$

$$E= 489250 \cdot 0,5 - 188732$$

$$E= 58935$$

Коефіцієнт повернення інвестицій ROSI показує, скільки гривень додаткового прибутку приносить одна гривня капітальних інвестицій на впровадження системи інформаційної безпеки:

$$ROSI = \frac{E}{K}$$

$$ROSI = \frac{58935}{21216}$$

$$ROSI = 2,8$$

Проект визнається економічно доцільним, якщо розрахунковий коефіцієнт

ефективності перевищує річний рівень прибутковості альтернативного варіанта:

$$ROSI > (N_{деп} - N_{інф})/100) \quad (3.20)$$

$$2,8> ((13-5)/100)$$

$$2,8> 0,08$$

Термін окупності капітальних інвестицій показує, за скільки років капітальні інвестиції окупляться за рахунок загального ефекту від впровадження системи інформаційної безпеки:

$$T_0 = \frac{K}{E} = \frac{1}{ROSI}, \text{ років}$$

$$T_0 = \frac{1}{2,8}$$

$$T_0 = 0,38 \text{ роки}$$

Висновки до третього розділу

У цьому розділі проведено детальний аналіз витрат на впровадження та експлуатацію захисних систем, що включає як капітальні, так і експлуатаційні витрати. Встановлено, що інвестиції в інформаційну безпеку є економічно обґрунтованими, оскільки вони дозволяють значно зменшити ризики втрат від потенційних кібератак. Проаналізовано загальні економічні вигоди, такі як зниження ймовірності витоку даних, скорочення простоїв у роботі та підвищення продуктивності співробітників завдяки надійному захисту інформаційних ресурсів.

Згідно з отриманими даними під час розрахунку економічної частини отримано, що капітальні затрати становлять 13101 грн, есплуатаційні- 203658 грн. При можливих річних збитках від атак на вузол корпоративної мережі органіції, що становлять 489250 грн, можна зрозуміти, що розробка елементів інформаційної безпеки є економічно доцільним.

Загальний ефект від впровадження системи становить 55629 грн. Згідно з коефіцієнтом повернення інвестицій ROSI, який становить 4,2, створенні елементи є цілком доцільними. Термін окупності елементів інформаційної безпеки становить 0,24 роки.

ВИСНОВОК

Підсумовуючи результати дослідження, можна стверджувати, що корпоративна електронна пошта на платформі Gmail, інтегрована з Google workspace , дає значні переваги для бізнесу з погляду безпеки та ефективності.

Завдяки використанню сучасних методів захисту, таких як протоколи SPF, DKIM і DMARC ризик несанкціонованого доступу та шкідливих атак значно знижується.

Згідно з отриманими даними, використання корпоративної електронної пошти через Google workspace не тільки підвищує рівень безпеки, а й сприяє підвищенню продуктивності праці та економічної ефективності бізнесу. Завдяки інтеграції інструментів штучного інтелекту та різних сервісів, Google workspace дає змогу оптимізувати робочий процес і скоротити витрати, пов'язані з кіберзлочинністю.

У світлі вищесказаного компаніям рекомендується перейти на використання корпоративної електронної пошти з відповідними налаштуваннями безпеки і постійно вдосконалювати свої заходи захисту для вирішення сучасних завдань кібербезпеки. З огляду на важливість захисту інформації, впровадження додаткових заходів безпеки, як двофакторна автентифікація (TFA) і запобігання втраті даних (DLP), є обов'язковим для сучасних компаній. Ці методи ускладнюють зловмисникам доступ до конфіденційної інформації та додатково посилюють захист корпоративної електронної пошти.

Протоколи безпеки SPF, DKIM і DMARC відіграють важливу роль у захисті корпоративної електронної пошти: SPF визначає, які сервери уповноважені надсилати електронні листи від імені домену, знижуючи ризик підміни адреси відправника; DKIM дає змогу електронним листам із цифровим підписом, щоб перевірити його достовірність і цілісність, а DMARC об'єднує можливості SPF і DKIM, щоб забезпечити контроль над неперевіреними листами.

Впровадження цих протоколів значно покращує захист електронної пошти від Фішингу та підробки. Для досягнення максимальної ефективності їх слід доповнити навчанням співробітників кібергігієни та регулярним оновленням

системи безпеки. Загалом, ці протоколи необхідні для забезпечення захисту електронної пошти компанії та зниження ризику кіберзлочинів.

Дослідження також показало, що економічна ефективність використання Google workspace перевищує початкові інвестиції, оскільки компанії отримують значну рентабельність інвестицій завдяки зниженню втрат від кіберзлочинів та підвищенню продуктивності праці. Крім того, можливість масштабування сервісу під потреби компанії дозволяє ефективно керувати ресурсами та забезпечувати стабільне зростання бізнесу.

ПЕРЕЛІК ПОСИЛАНЬ

1 Phishing email attack statistics and facts for 2019–2024 URL: https://www.comparitech.com/blog/vpn-privacy/Phishing-statistics- facts/ (дата звернення: 29.05.2024)

2 Call Me Ishmael - All About Whaling Scams: URL: https://digital.va.gov/general/call-me-ishmael-all-about-whaling-scams// (дата звернення: 29.05.2024)

3 State of Phishing & Online Scams: URL: https://bolster.ai/blog/2024-state-of-Phishing-statistics-online-scams/ (дата звернення: 29.05.2024)

4 Phishing Attack Statistics You Should Know in 2024: URL: https://sprinto.com/blog/Phishing-statistics// (дата звернення: 30.05.2024)

5 Types of Email Attacks: URL: https://www.geeksforgeeks.org/types-of-email-attacks/(дата звернення: 30.05.2024)

6 Cybersecurity Statistics and Trends: веб-сайт. URL: https://www.varonis.com/blog/cybersecurity-statistics(дата звернення: 30.05.2024)

7 PHISHING ACTIVITY TRENDS REPORT: URL: https://docs.apwg.org/reports/apwg_trends_report_q2_2023.pdf (дата звернення: 01.06.2024)

8 THE LITTLE BLACK BOOK OF SCAMS: URL: https://www.yrp.ca/en/crime-prevention/resources/Little-Black-Book-Scams- e.pdf (дата звернення: 01.06.2024)

9 What is a Whaling Attack: URL: https://www.kaspersky.com/resource-center/definitions/what-is-a-whaling-attack (дата звернення: 01.06.2024)

10 Spam statistic (2024): URL: https://www.emailtooltester.com/en/blog/spam-statistics/?rel=nofollow (дата звернення: 02.06.2024)

11 Defining Ransomware: URL: https://www.knowbe4.com/ransomware (дата звернення: 02.06.2024)

12 2019 INTERNET CRIME REPORT: URL: https://www.ic3.gov/Media/PDF/AnnualReport/2019_IC3Report.pdf (дата звернення:

03.06.2024)

13 2020 INTERNET CRIME REPORT: URL: https://www.ic3.gov/media/PDF/AnnualReport/2020_IC3ElderFraud Report.pdf (дата звернення: 03.06.2024)

14 Програма-вимагач: як розпізнати їх та убезпечити своє підприємство? : URL: https://ukeywaf.com/programa-vymagach-yak-rozpiznaty-yih-ta-ubezpechyty- svoye-pidpryyemstvo/ (дата звернення: 03.06.2024)

15 2023 INTERNET CRIME REPORT: URL: https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf (дата звернення: 03.06.2024)

16 Top Phishing Statistics for 2024: URL: https://www.stationx.net/Phishing-statistics/(дата звернення: 04.06.2024)

17 How to set up a corporate e-mail address on your own domain: URL: https://www.ispmanager.com/news/how-to-set-up-a-corporate-e-mail- address-on-your-own-domain (дата звернення: 04.06.2024)

11 How Long Does It Take for a Hacker to Crack a Password: URL: https://tech.co/password-managers/how-long-hacker-crack-password (дата звернення: 08.06.2024)

12 Allowlists, denylists, and approved senders URL: https://support.google.com/a/answer/60752 (дата звернення: 09.06.2024)

13 Google workspace Security Best Practices for Ultimate G Suite Security: URL: https://underdefense.com/blog/google-workspace-security-best-practices-for-ultimate-g-suite-security/ (дата звернення: 09.06.2024)

14 Understanding Google workspace Security Settings & Features: URL: https://promevo.com/blog/google-workspace-security-settings-and-features

15 What Is Sender Policy Framework (SPF): URL: https://www.proofpoint.com/us/threat-reference/spf (дата звернення: 09.06.2024)

16 What Is DKIM: URL: https://www.proofpoint.com/us/threat-reference/dkim (дата звернення: 09.06.2024)

17 What Is DMARC: URL: https://www.proofpoint.com/us/threat-reference/dmarc (дата звернення: 09.06.2024)

18 What is SMTP: URL: https://aws.amazon.com/what-is/smtp/?nc1=h_ls (дата звернення: 11.06.2024)

19 An ultimate guide to email infrastructure: URL: https://mailtrap.io/blog/email-infrastructure/ (дата звернення: 11.06.2024)

20 What is Email Spoofing: URL: https://fortinet.com/resources/cyberglossary/email-spoofing (дата звернення: 11.06.2024)

21 Business Email Compromise: The $50 Billion Scam: URL: https://www.ic3.gov/Media/Y2023/PSA230609 (дата звернення: 11.06.2024)

22 Infographics Title : DMARC Statistics: URL: https://medium.com/@d.marc.sub.mission2022/infographics-title-dmarc- statistics-abfb8ce0eae0 (дата звернення: 11.06.2024)

23 How to Create Cybersecurity Training for Employees URL: https://www.edgepointlearning.com/blog/cyber-security-training/ (дата звернення: 13.06.2024)

24 What is DMARC and how does it work: URL: https://www.mailjet.com/blog/deliverability/what-is-dmarc/ (дата звернення: 13.06.2024)

25 Що таке наскрізне шифрування (E2EE) : URL: https://www.cloudflare.com/ru-ru/learning/privacy/what-is-end-to-end-encryption/ (дата звернення: 13.06.2024)

26 Створення приватного та публічного RSA ключа : URL: https://cryptography.io/en/latest/hazmat/primitives/asymmetric/serialization/ (дата

звернення: 14.06.2024)

27 Small Python script to quick test DMARC DKIM and SPF: URL: recordshttps://www.thierolf.org/posts/small-python-script-to-quick-test-dmarc-dkim-and-spf-records/ (дата звернення: 14.06.2024)

28 DNS resorvel module: URL: https://dnspython.readthedocs.io/en/latest/_modules/dns/resolver.html (дата звернення: 14.06.2024)

ДОДАТОК А. відомість матеріалів кваліфікаційної роботи

№	Формат	Найменування	Кількість листів	Примітка
1	А4	Реферат	2	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	2	
4	А4	Вступ	2	
5	А4	1 Розділ	21	
6	А4	2 Розділ	30	
7	А4	3 Розділ	10	
8	А4	Висновки	2	
9	А4	Перелік посилань	3	
10	А4	Додаток А	1	
11	А4	Додаток Б	1	
12	А4	Додаток В	5	
13	А4	Додаток Г	1	
14	А4	Додаток Д	1	

ДОДАТОК Б. Перелік документів на оптичному носії

ПіцикІВ_125-20-2_Кр.docx

ПіцикІВ_125-20-2_Кр.Pdf

Презентація.pptx

ПіцикІВ_125-20-2_Кр. p7s

ДОДАТОК В. Розроблені коди кваліфікаційної роботи

Код шифрування та дешифрування:

Шифрування:

```
import smtplib
from email.mime.text import MIMEText
from email.mime.multipart import MIMEMultipart
from cryptography.hazmat.primitives.asymmetric import rsa
from cryptography.hazmat.primitives import serialization
from cryptography.hazmat.primitives.asymmetric import padding
from cryptography.hazmat.primitives import hashes

private_key = rsa.generate_private_key(
    public_exponent=65537,
    key_size=2048,
)
public_key = private_key.public_key()

public_pem = public_key.public_bytes(
    encoding=serialization.Encoding.PEM,
    format=serialization.PublicFormat.SubjectPublicKeyInfo
)
with open('public_key.pem', 'wb') as f:
    f.write(public_pem)

private_pem = private_key.private_bytes(
    encoding=serialization.Encoding.PEM,
    format=serialization.PrivateFormat.PKCS8,
    encryption_algorithm=serialization.NoEncryption()
)
with open('private_key.pem', 'wb') as f:
    f.write(private_pem)

message = b'This is a secret message.'

encrypted_message = public_key.encrypt(
    message,
    padding.OAEP(
        mgf=padding.MGF1(algorithm=hashes.SHA256()),
        algorithm=hashes.SHA256(),
        label=None
    )
```

```
)
sender_email = "pytsyk.i.v@gmail.com"
receiver_email = "Pitsyk.I.V@nmu.one"
password = "**** **** **** ****"

msg = MIMEMultipart()
msg['From'] = sender_email
msg['To'] = receiver_email
msg['Subject'] = "Зашифроване посилання"

msg.attach(MIMEText(encrypted_message.hex(), 'plain'))

try:
    server = smtplib.SMTP('smtp.gmail.com', 587)
    server.starttls()
    server.login(sender_email, password)
    server.sendmail(sender_email, receiver_email, msg.as_string())
    print("Лист успішно відправленний")
except Exception as e:
    print(f"Помилка: {e}")
finally:
    server.quit()
```

Дешифрування:

```
from cryptography.hazmat.primitives import serialization
from cryptography.hazmat.primitives.asymmetric import padding
from cryptography.hazmat.primitives import hashes

with open('private_key.pem', 'rb') as f:
    private_key = serialization.load_pem_private_key(
        f.read(),
        password=None,
    )
with open('Encrypted Message.txt', 'r') as f:
    encrypted_message_hex = f.read().strip()
encrypted_message = bytes.fromhex(encrypted_message_hex)

decrypted_message = private_key.decrypt(
    encrypted_message,
    padding.OAEP(
        mgf=padding.MGF1(algorithm=hashes.SHA256()),
        algorithm=hashes.SHA256(),
        label=None
```

```
    )
)
print("Розшифроване посилання:\n", decrypted_message.decode('utf-8'))
```

Код перевірки протоколів безпеки:

Java Script:

```
function doGet() {
  var threads = GmailApp.getInboxThreads(0, 10);
  var messages = GmailApp.getMessagesForThreads(threads);
  var emails = [];

  for (var i = 0; i < messages.length; i++) {
    for (var j = 0; j < messages[i].length; j++) {
      var message = messages[i][j];
      var from = message.getFrom();
      var body = message.getPlainBody();
      emails.push({
        from: from,
        body: body
      });
    }
  }

  return
ContentService.createTextOutput(JSON.stringify(emails)).setMimeType(ContentService.MimeTyp
e.JSON);
}
```

Python:

```
import requests
import dns.resolver
import re

script_url = 'https://script.google.com/macros/s/'
def get_senders(script_url):
    response = requests.get(script_url)
    if response.status_code == 200:
        return response.json()
    else:
        raise Exception('Помилка при отриманні інформації')

def extract_domain(email):
    match = re.search(r'@([\w.-]+)', email)
    return match.group(1) if match else None

def check_dmarc_spf_for_senders(script_url):
    senders = get_senders(script_url)
    results = {}
    for sender in senders:
```

```
            domain = extract_domain(sender)
            if domain:
                print(f"Перевірка домену: {domain}")
                dmarc_record = get_dmarc_record(domain)
                spf_record = get_spf_record(domain)
            else:
                print(f"Неправильний формат електронної пошти: {sender}")

    return results

def get_dmarc_record(domain):
    try:
        dmarc_domain = '_dmarc.' + domain
        answers = dns.resolver.resolve(dmarc_domain, 'TXT')
        return '\n'.join([rdata.to_text() for rdata in answers])
    except dns.resolver.NoAnswer:
        return ' DMARC запис не знайдено'
    except dns.resolver.NXDOMAIN:
        return 'DMARC домен не існує'
    except Exception as e:
        return f'Error: {e}'


def get_spf_record(domain):
    try:
        answers = dns.resolver.resolve(domain, 'TXT')
        for rdata in answers:
            if 'v=spf1' in rdata.to_text():
                return rdata.to_text()
        return 'запис SPF не знайдено'
    except dns.resolver.NoAnswer:
        return 'запис SPF не знайдено'
    except dns.resolver.NXDOMAIN:
        return 'SPF домен не існує'
    except Exception as e:
        return f'Помилка: {e}'

results = check_dmarc_spf_for_senders(script_url)
for domain, records in results.items():
    print(f"Domain: {domain}")
    print(f"DMARC: {records['dmarc']}")
    print(f"SPF: {records['spf']}")
    print("\n")
```

Код сканування вкладень електронної пошти:

```
import imaplib
import email
import requests

IMAP_SERVER = "imap.gmail.com"
EMAIL_ACCOUNT = "pytsyk.i.v@gmail.com"
PASSWORD = "**** **** **** ****"
API_KEY = '572d16fe6c372fbe3eb7f518...'

def connect_to_mail():
    mail = imaplib.IMAP4_SSL(IMAP_SERVER)
    mail.login(EMAIL_ACCOUNT, PASSWORD)
    return mail

def fetch_attachments(mail):
    mail.select('inbox')
    result, data = mail.search(None, 'ALL')
    mail_ids = data[0].split()
```

```
    attachments = []

    for mail_id in mail_ids:
        result, msg_data = mail.fetch(mail_id, '(RFC822)')
        raw_email = msg_data[0][1]
        msg = email.message_from_bytes(raw_email)

        for part in msg.walk():
            if part.get_content_maintype() == 'multipart':
                continue
            if part.get('Content-Disposition') is None:
                continue
            file_name = part.get_filename()
            if bool(file_name):
                attachments.append((file_name, part.get_payload(decode=True)))

    return attachments


def scan_attachment(file_content, file_name, api_key):
    url = 'https://www.virustotal.com/vtapi/v2/file/scan'
    files = {'file': (file_name, file_content)}
    params = {'apikey': api_key}
    response = requests.post(url, files=files, params=params)
    return response.json()
def save_scan_result(file_name, result):
    with open("scan_results.txt", "a") as file:
        file.write(f"Просканировано {file_name}: {result}\n")


def main():
    mail = connect_to_mail()
    attachments = fetch_attachments(mail)

    for file_name, file_content in attachments:
        result = scan_attachment(file_content, file_name, API_KEY)
        save_scan_result(file_name, result)
        print(f"Scanned {file_name}: {result}")


if __name__ == "__main__":
    main()
```

ДОДАТОК Г. Відгук керівника економічного розділу

Відгук керівника економічного розділу:

Економічний розділ виконаний відповідно до вимог, які ставляться до кваліфікаційних робіт, та заслуговує на оцінку 90 б

Керівник розділу _____ доц. Пілова Д.П.

(підпис) (ініціали, прізвище)

ДОДАТОК Д. Відгук керівника кваліфікаційної роботи

В І Д Г У К

на кваліфікаційну роботу студента групи 125-20-2

Піцика Івана Віталійовича

на тему: «Методи реалізації захисту корпоративної пошти на платформі Gmail.»

Пояснювальна записка складається зі вступу, трьох розділів і висновків, викладених 74 на сторінках.

Метою кваліфікаційної роботи є дослідження сучасних підходів до захисту корпоративної електронної пошти Google workspace і розробка комплексу ефективних методів забезпечення інформаційної безпеки

Тема кваліфікаційної роботи безпосередньо пов'язана з об'єктом діяльності бакалавра спеціальності 125 «Кібербезпека». Для досягнення поставленої мети в кваліфікаційній роботі вирішуються наступні задачі: розробка методів захисту інформаціїї корпоративної пошти шляхом впровадження таких як двофакторна аутентифікація, шифрування листів та протоколи безпеки

Практичне значення результатів кваліфікаційної роботи полягає у розробці та впровадженні сучасних технологій захисту інформації, за допомогою яких організація зможе мінімізувати ризики кіберзагроз та зменшити потенційні економічні збитки від атак на корпоративну пошту

Оформлення пояснювальної записки до кваліфікаційної роботи виконано з незначними відхиленнями від стандартів.

За час дипломування Піцик І.В. проявив себе фахівцем, здатним самостійно вирішувати поставлені задачі та заслуговує присвоєння кваліфікації бакалавра за спеціальністю 125 Кібербезпека, освітньо-професійна програма «Кібербезпека».

Рівень запозичень у кваліфікаційній роботі не перевищує вимог "Положення про систему виявлення та запобігання плагіату".

Кваліфікаційна робота заслуговує оцінки «_____».

Керівник кваліфікаційної роботи к.ф.-м.н., проф. Гусєв О.Ю.

Керівник спец. розділу ст викл. Тимофєєв Д.С.